# LevelOne

# WBR-5400

## MIMO Wireless 1W,4L Broadband Router

# User`s Manual

Ver 1.00-0512

## Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

## Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

## FCC Interference Statement

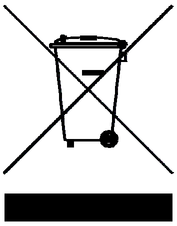
This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

## CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

**The specification is subject to change without notice.**

# Table of Contents



# Chapter 1 Introduction

Congratulations on your purchase of this outstanding LevelOne WBR-5400, 11g MIMO Wireless Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

## Functions and Features

### Router Basic functions

- **Auto-sensing Ethernet Switch**
  Equipped with a 4-port auto-sensing Ethernet switch.
- **WAN type supported**
  The router supports some WAN types, Static, Dynamic, PPPoE , PPTP ,L2TP, and Dynamic IP with Road Runner.
- **Firewall**
  All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**
  All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**
  Configurable through any networked computer's web browser using Netscape or Internet Explorer.
- **Virtual Server supported**
  Enable you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **User-Definable Application Sensing Tunnel**
  User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.
- **DMZ Host supported**
  Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.
- **Statistics of WAN Supported**
  Enables you to monitor inbound and outbound packets

## Wireless functions

- **High speed for wireless LAN connection**

  Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

- **Roaming**

  Provides seamless roaming within the IEEE 802.11b (11M) and IEEE 802.11g (54M) WLAN infrastructure.

- **IEEE 802.11b compatible (11M)**

  Allowing inter-operation among multiple vendors.

- **IEEE 802.11g compatible (54M)**

  Allowing inter-operation among multiple vendors.

- **MIMO with new MRC technology**

  The farther away, the more advantage -- up to 6 times faster than standard Wireless-G (802.11g) in certain distance and circumstances.

  MIMO technology also reduces dead spots in coverage area

- **Enhanced wireless coverage and fully compatible with 802.11g and 802.11b.**

## Security functions

- **Packet filter supported**

  **Packet Filter** allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Domain Filter Supported**

  Let you prevent users under this device from accessing specific URLs.

- **URL Blocking Supported**

  URL Blocking can block hundreds of websites connection by simply a **keyword**.

- **VPN Pass-through**

  The router also supports VPN pass-through.

- **802.1X supported**

  When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

- **Support WPA-PSK and WPA**

  When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service

- **SPI Mode Supported**

When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.

- **DoS Attack Detection Supported**

  When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

### Advanced functions

- **System time Supported**

  Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

  The router can send its info by mail.

- **Dynamic dns Supported**

  At present,the router has 3 ddns.dyndns,TZO.com and dhs.org.

- **SNMP Supported**

  The router supports basic SNMP function.

- **Routing Table Supported**

  Now, the router supports static routing.

- **Schedule Rule supported**

  Customers can control some functions, like virtual server and packet filters when to access or when to block.

### Other functions

- **UPNP (Universal Plug and Play)Supported**

  The router also supports this function. The applications: X-box, Msn Messenger.

## Packing List

- Wireless broadband router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable
- QIG

# Chapter 2 Hardware Installation

## 2.1 Panel Layout

### 2.1.1. Front Panel

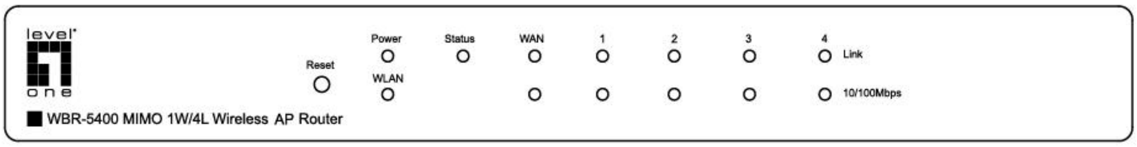


Figure 2-1 Front Panel

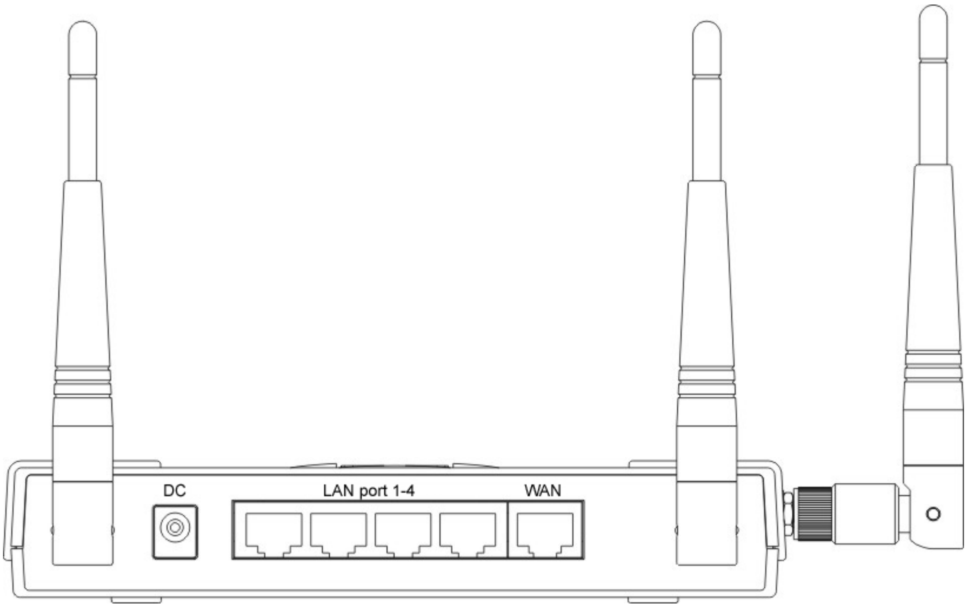
LED:

| LED | Function | Color | Status | Description |
|---|---|---|---|---|
| POWER | Power indication | Green | On | Power is being applied to this product. |
| STATUS | System status indicators | Green | Blinking | STATUS is flashed once per second to indicate system is alive. |
| WAN | WAN port activity | Green | On | The WAN port is linked. |
| | | | Blinking | The WAN port is sending or receiving data. |
| WLAN | Wireless activity | Green | Blinking | Sending or receiving data via wireless |
| Link. 1~4 | Link status | Green | On | An active station is connected to the corresponding LAN port. |
| | | | Blinking | The corresponding LAN port is sending or receiving data. |
| 10/100 Mbps | Data Rate | Green | On | Data is transmitting in 100Mbps on the corresponding LAN port. |
| Reset | Reset | | | To reset system settings to factory defaults |

### 2.1.2. Rear Panel

Ports:

| Port | Description |
|---|---|
| **PWR(DC)** | Power inlet |
| **WAN** | the port where you will connect your cable (or DSL) modem or Ethernet router. |
| **Port 1-4** | the ports where you will connect networked computers and other devices. |



## 2.2 Procedure for Hardware Installation

2. **Decide where to place your Wireless Broadband Router**

   You can place your WBR-5400, Wireless Broadband Router, on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

2. **Setup LAN connection**

   **a.** Wired LAN connection: connects an Ethernet cable from your computer’s Ethernet port to one of the LAN ports of this product.

   **b.** Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

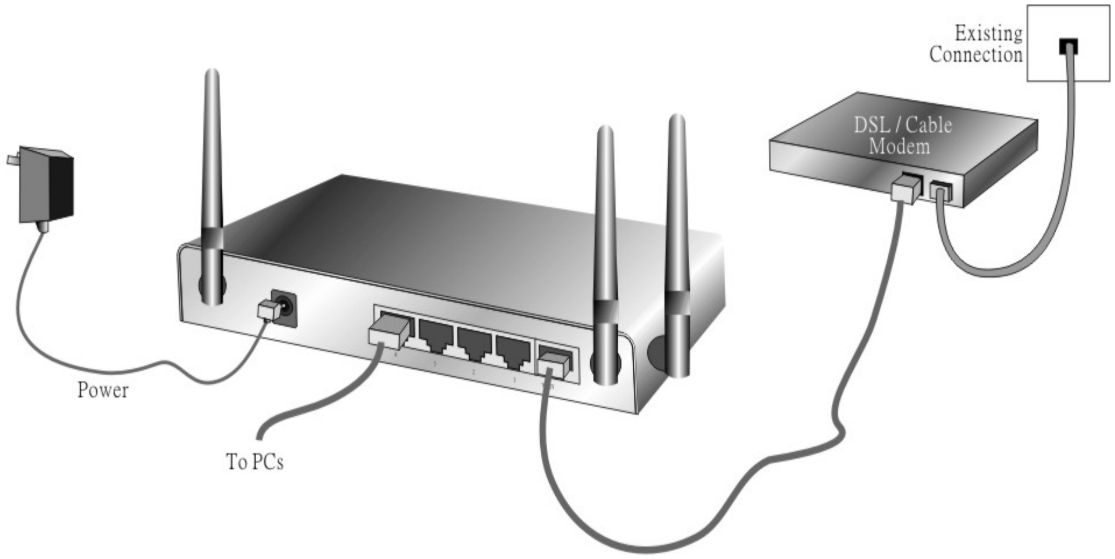


Figure 2-3 Setup of LAN and WAN connections for this product.

3. **Setup WAN connection**

   Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

4. **Power on**

   Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators STATUS will be lighted ON for about 10 seconds, and then STATUS will be flashed 3 times to indicate that the self-test operation has finished. Finally, the STATUS will be continuously flashed once per second to indicate that this product is in normal operation.

# Chapter 3 Network Settings and Software Installation

To use WBR-5400 correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (98SE/ME/2000/XP )

## 3.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,
2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

```
ping 192.168.123.254
```

If the following messages appear:

```
Pinging 192.168.123.254 with 32 bytes of data:
Reply from 192.168.123.254: bytes=32 time=2ms TTL=64
```

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

```
Pinging 192.168.123.254 with 32 bytes of data:
Request timed out.
```

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

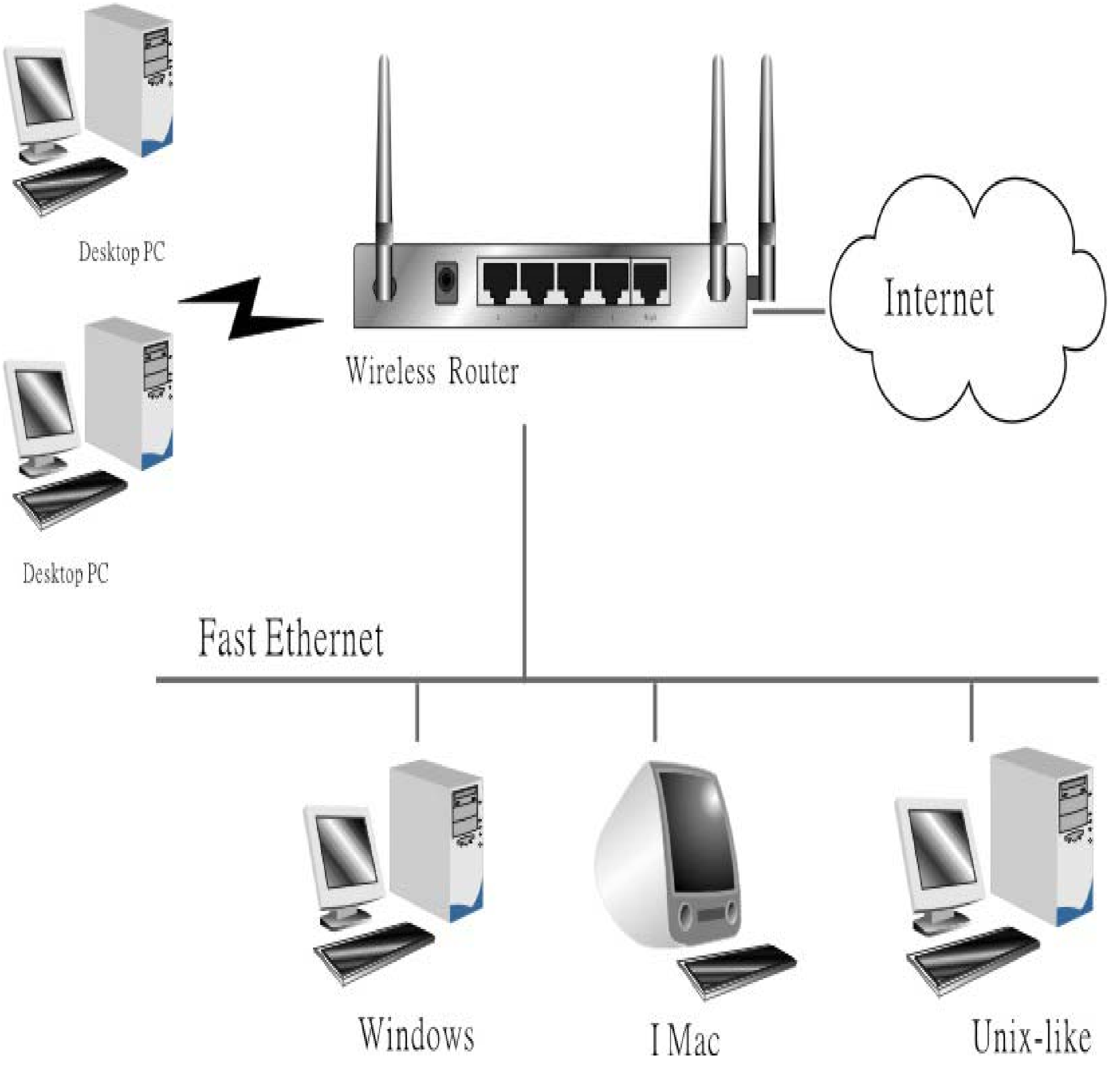
   **Tip**: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

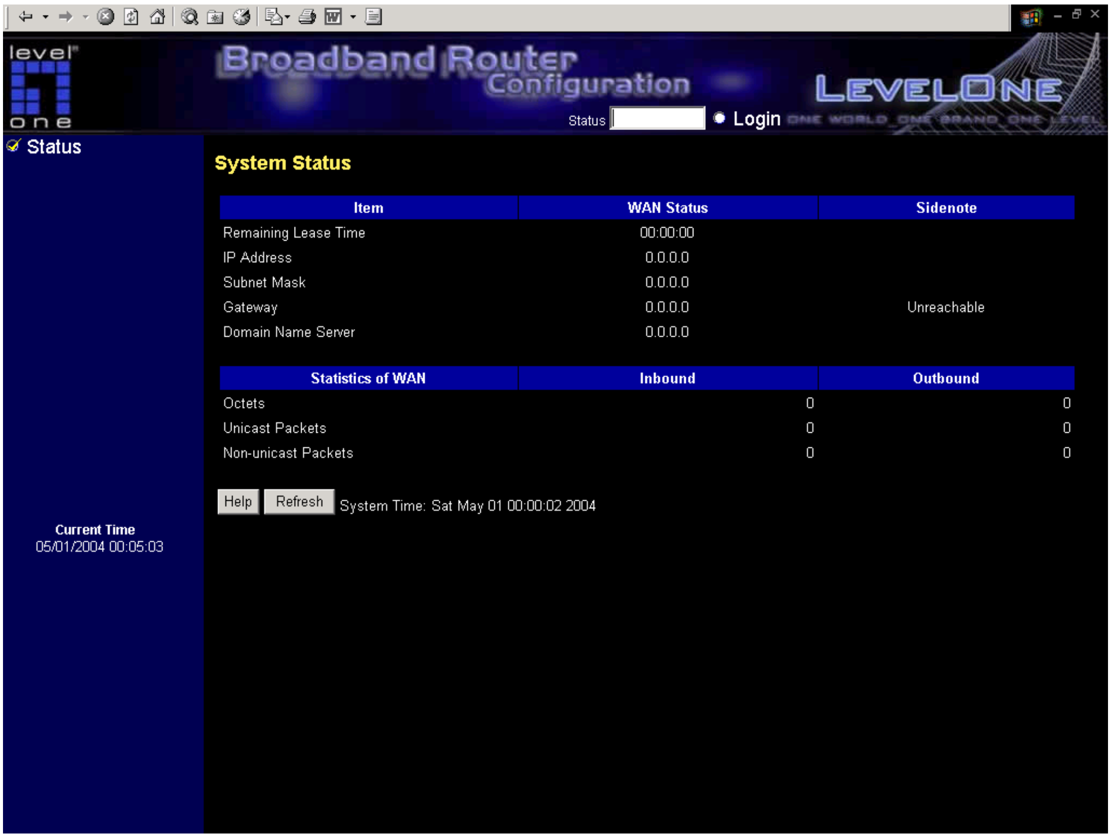
   **Tip**: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

# Chapter 4    Configuring Wireless Broadband Router

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



## 4.1 Start-up and Log in



System Status

| Item | WAN Status | Sidenote |
|---|---|---|
| Remaining Lease Time | 00:00:00 | |
| IP Address | 0.0.0.0 | |
| Subnet Mask | 0.0.0.0 | |
| Gateway | 0.0.0.0 | Unreachable |
| Domain Name Server | 0.0.0.0 | |

| Statistics of WAN | Inbound | Outbound |
|---|---|---|
| Octets | 0 | 0 |
| Unicast Packets | 0 | 0 |
| Non-unicast Packets | 0 | 0 |

System Time: Sat May 01 00:00:02 2004

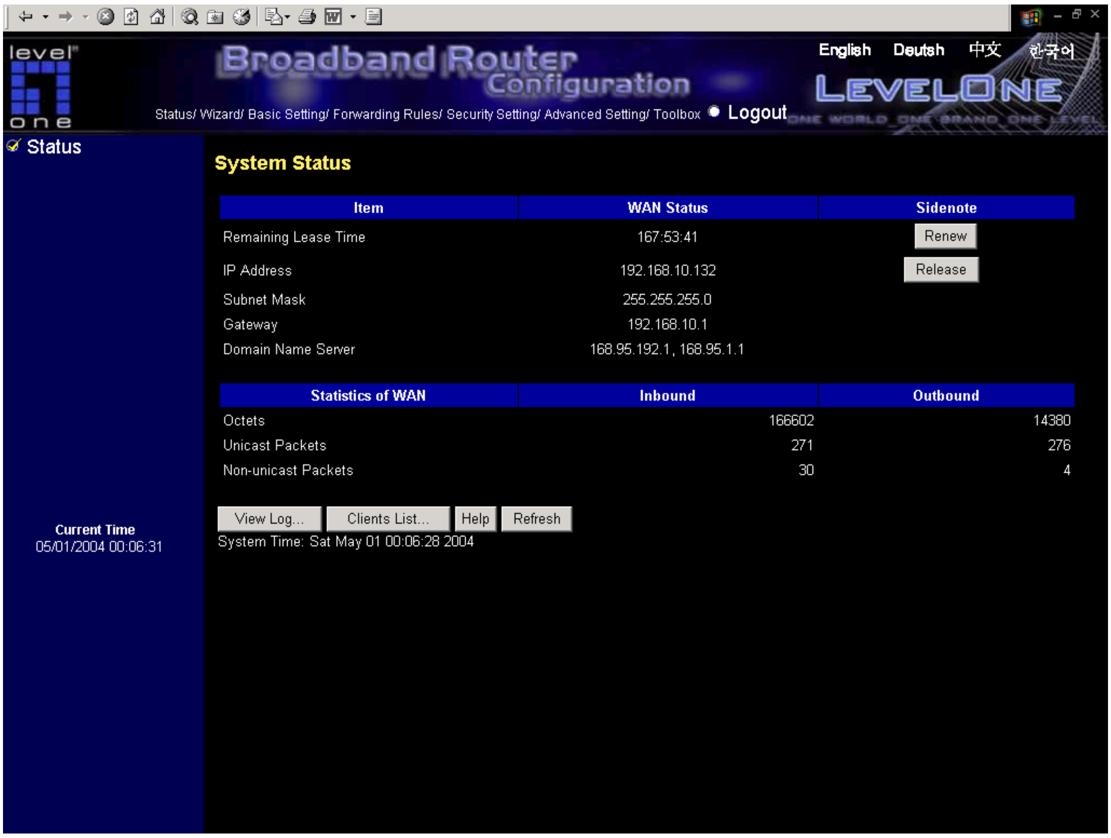
Current Time
05/01/2004 00:05:03

Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: **http://192.168.123.254**.

After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter the system password (the factory setting is "**admin**") in the **System Password** field and click on the **Log in** button. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.

## 4.2 Status


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Status
Renew
Release
View Log...
Clients List...
Help
Refresh

System Status

| Item | WAN Status | Sidenote |
|---|---|---|
| Remaining Lease Time | 167:53:41 | Renew |
| IP Address | 192.168.10.132 | Release |
| Subnet Mask | 255.255.255.0 | |
| Gateway | 192.168.10.1 | |
| Domain Name Server | 168.95.192.1, 168.95.1.1 | |

| Statistics of WAN | Inbound | Outbound |
|---|---|---|
| Octets | 166602 | 14380 |
| Unicast Packets | 271 | 276 |
| Non-unicast Packets | 30 | 4 |

System Time: Sat May 01 00:06:28 2004

Current Time
05/01/2004 00:06:31

This option provides the function for observing this product’s working status:

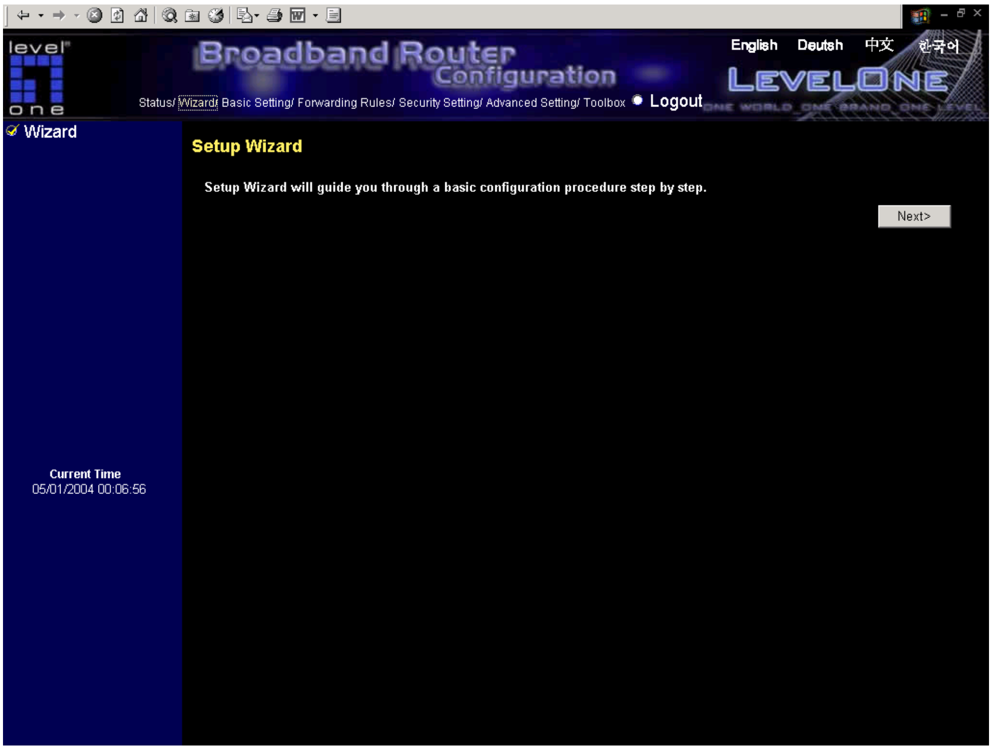
A. WAN Port Status.

If the WAN port is assigned a dynamic IP, there may appear a “**Renew**” or “**Release**” button on the Sidenote column. You can click this button to renew or release IP manually.

B. Statistics of WAN: enables you to monitor inbound and outbound packets

**Note:** After successful login, you can switch the language in the Web-based user interface. There are four languages available, which are English, Deutsh, Chinese, and Korean. Please select the language by clicking the option on the top-right corner.

## 4.3 Wizard

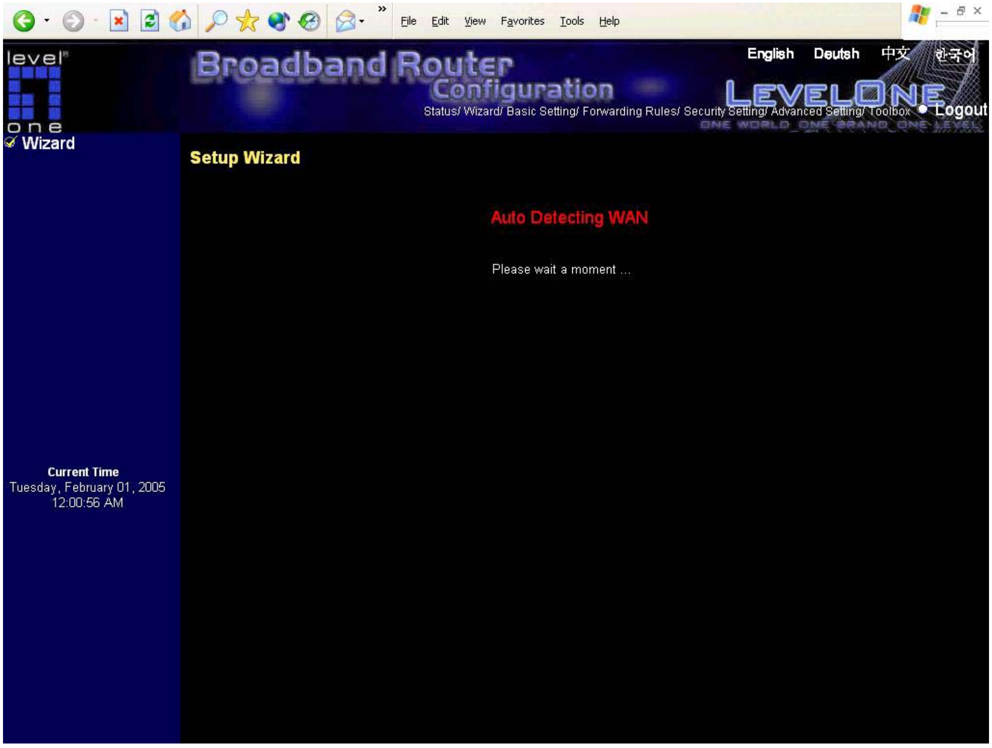

level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Wizard
Next>

Setup Wizard

Setup Wizard will guide you through a basic configuration procedure step by step.

Current Time
05/01/2004 00:06:56

Setup Wizard will guide you through a basic configuration procedure step by step.Press **”Next >”**


File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Wizard

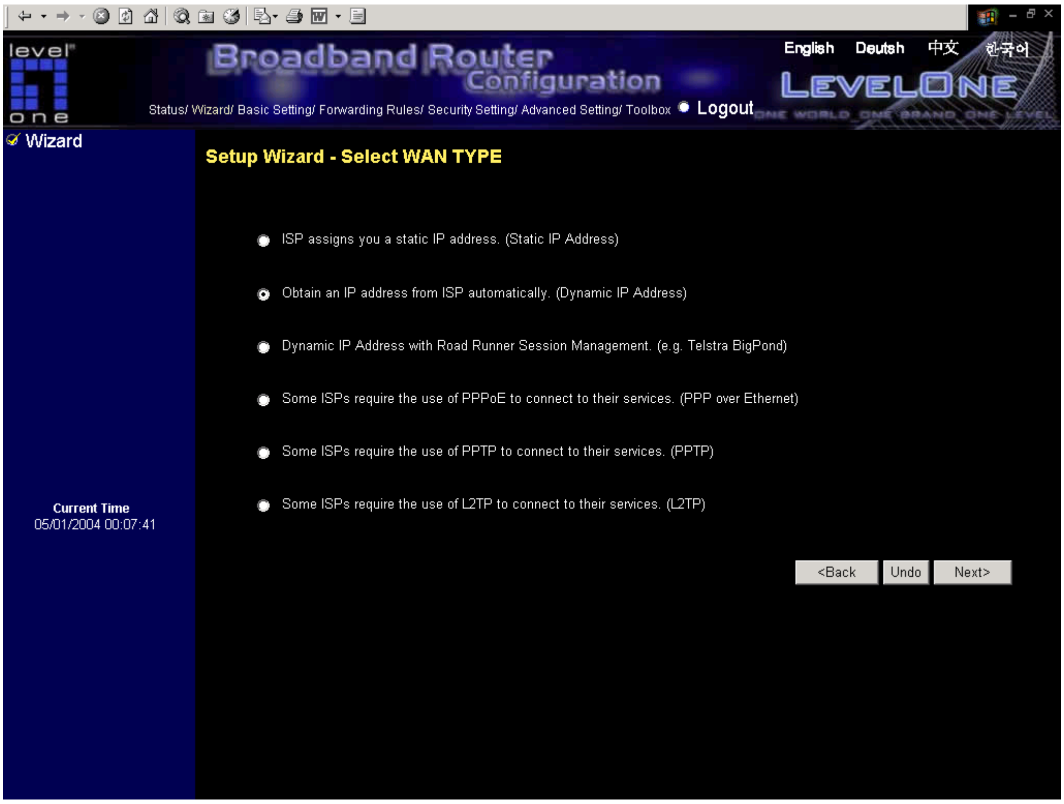
Setup Wizard

Auto Detecting WAN

Please wait a moment ...

Current Time
Tuesday, February 01, 2005
12:00:56 AM

Setup Wizard will automatically detect your WAN type. If WAN type can not be detected successfully, “Dynamic IP Address” will be assigned.


level one
Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
English
Deutsh
中文
한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Wizard
<Back
Undo
Next>

Setup Wizard - Select WAN TYPE

- ○ ISP assigns you a static IP address. (Static IP Address)
- ● Obtain an IP address from ISP automatically. (Dynamic IP Address)
- ○ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)
- ○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)
- ○ Some ISPs require the use of PPTP to connect to their services. (PPTP)
- ○ Some ISPs require the use of L2TP to connect to their services. (L2TP)

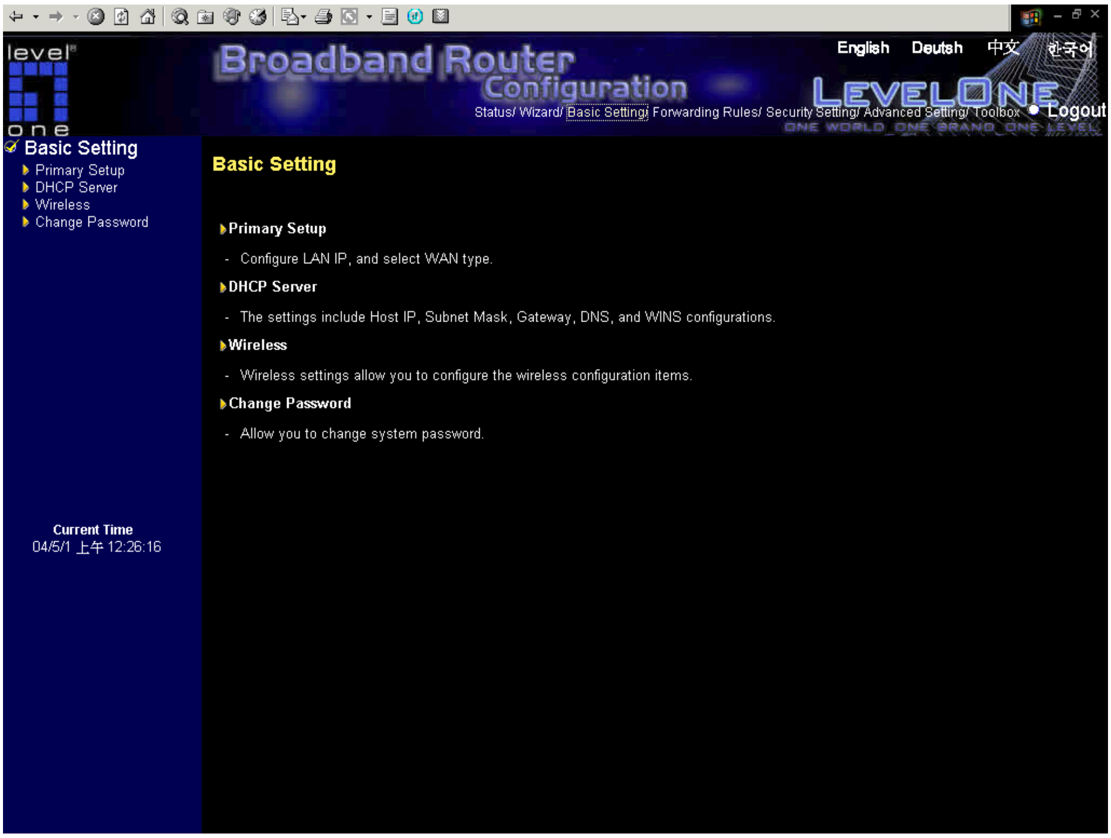
Current Time
05/01/2004 00:07:41

**Setup Wizard - Select WAN Type**: For detail settings, please refer to **4.4.1 primary setup.**

For the rest of the steps, Setup Wizard will guide you through a basic configuration.

.Press **"Next >"**

## 4.4 Basic Setting



Broadband Router Configuration
English
Deutsh
中文
한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Current Time
04/5/1 上午 12:26:16

**Basic Setting**

**Primary Setup**

- Configure LAN IP, and select WAN type.

**DHCP Server**

- The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.

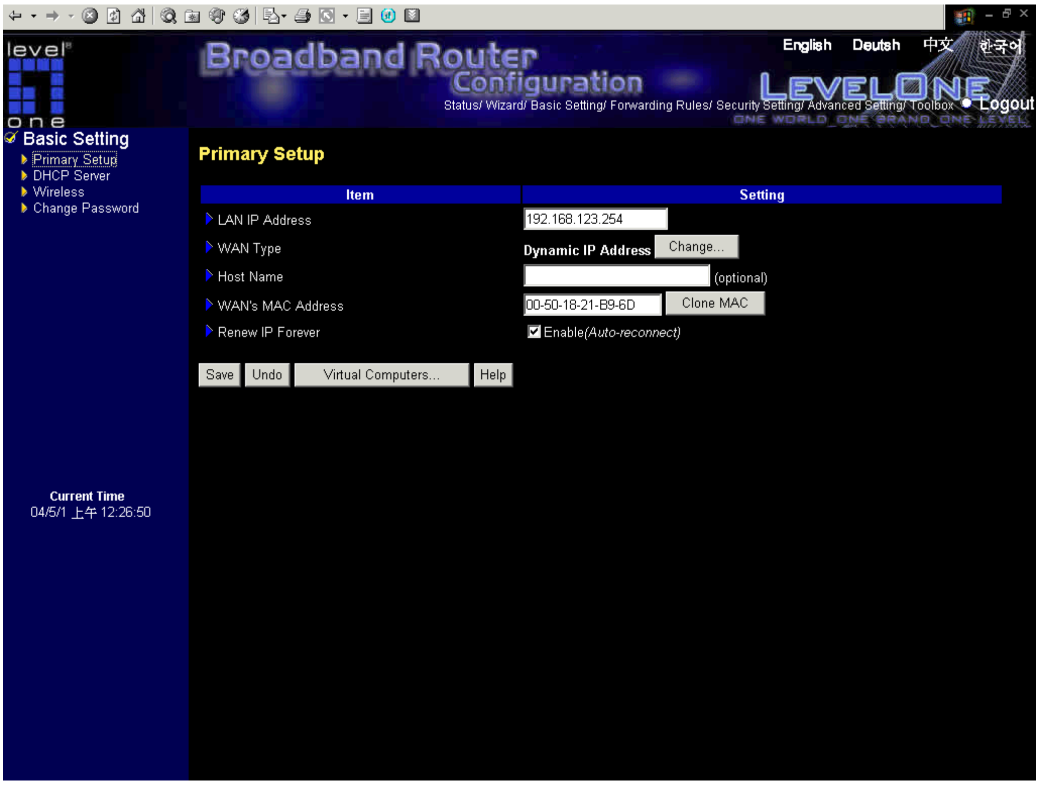
**Wireless**

- Wireless settings allow you to configure the wireless configuration items.

**Change Password**

- Allow you to change system password.

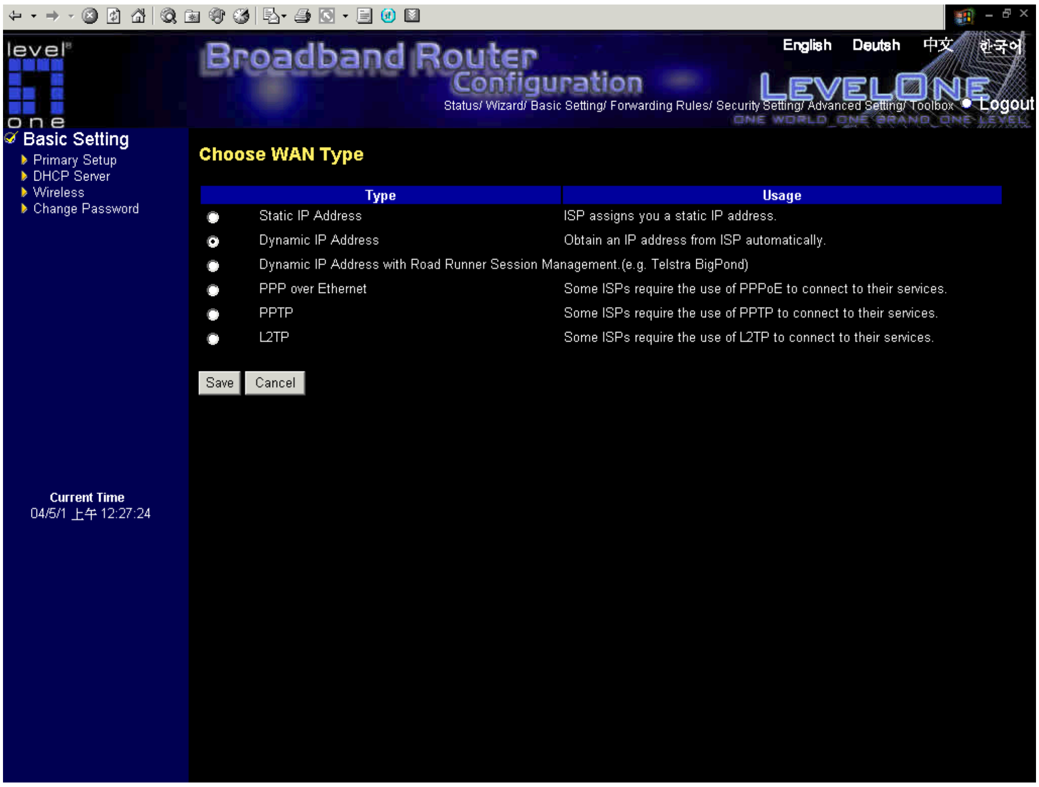
## 4.4.1 Primary Setup – WAN Type, Virtual Computers



Primary Setup

| Item | Setting |
|---|---|
| LAN IP Address | 192.168.123.254 |
| WAN Type | Dynamic IP Address [Change...] |
| Host Name | (optional) |
| WAN's MAC Address | 00-50-18-21-B9-6D [Clone MAC] |
| Renew IP Forever | ☑ Enable(*Auto-reconnect*) |

Press **"Change"**



Choose WAN Type

| | Type | Usage |
|---|---|---|
| ○ | Static IP Address | ISP assigns you a static IP address. |
| ● | Dynamic IP Address | Obtain an IP address from ISP automatically. |
| ○ | Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond) | |
| ○ | PPP over Ethernet | Some ISPs require the use of PPPoE to connect to their services. |
| ○ | PPTP | Some ISPs require the use of PPTP to connect to their services. |
| ○ | L2TP | Some ISPs require the use of L2TP to connect to their services. |

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address**: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type**: WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:
   A. Static IP Address: ISP assigns you a static IP address.
   B. Dynamic IP Address: Obtain an IP address from ISP automatically.
   C. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
   D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
   E. PPTP: Some ISPs require the use of PPTP to connect to their services.

#### 4.4.1.1 Static IP Address

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

#### 4.4.1.2 Dynamic IP Address

1. Host Name: optional. Required by some ISPs, for example, @Home.
2. Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

#### 4.4.1.3 Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)

1 LAN IP Address is the IP address of this product. It must be the default gateway of your computers.

2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!

3. Host Name: optional. Required by some ISPs, e.g. @Home.

4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

#### 4.4.1.4 PPP over Ethernet

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.

### 4.4.1.5 PPTP

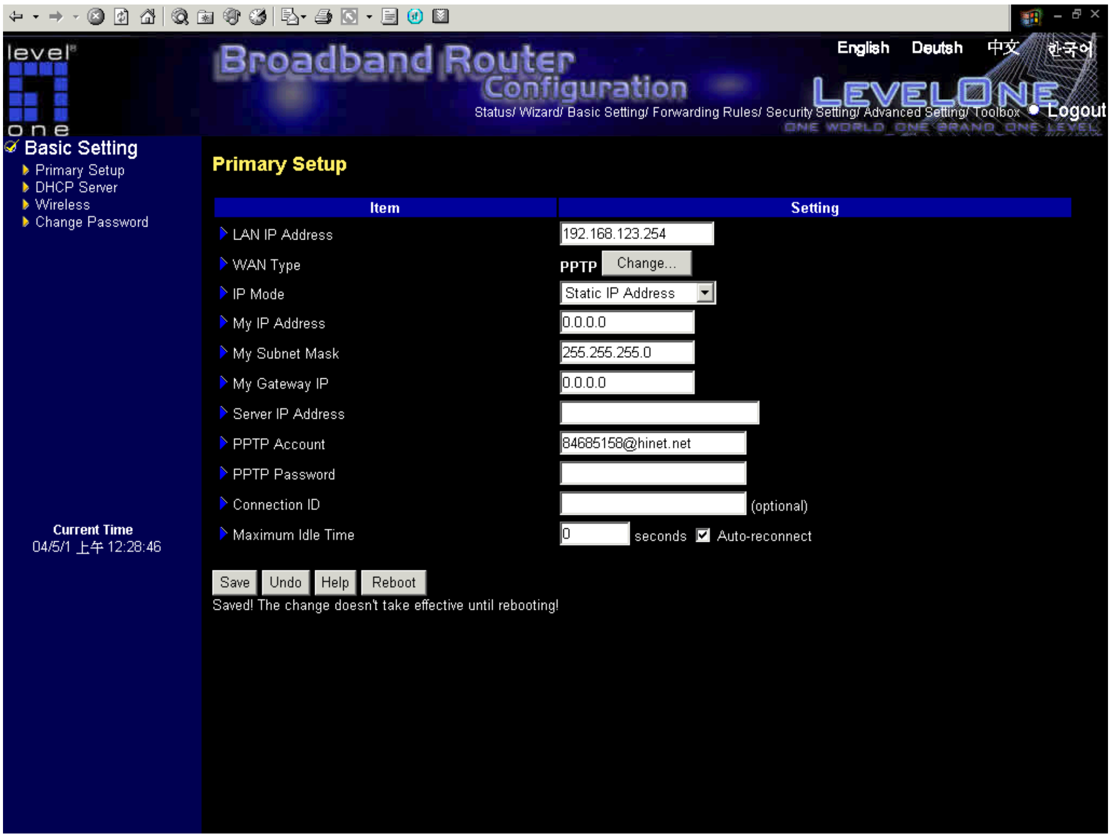
1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

2. Server IP Address: the IP address of the PPTP server.

3. PPTP Account and Password: the account and password your ISP assigned to you. If you don'twant to change the password, keep it empty.

3. Connection ID: optional. Input the connection ID if your ISP requires it.

4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.


Broadband Router Configuration
English
Deutsh
中文
한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
Help
Reboot

Current Time
04/5/1 上午 12:28:46

Primary Setup

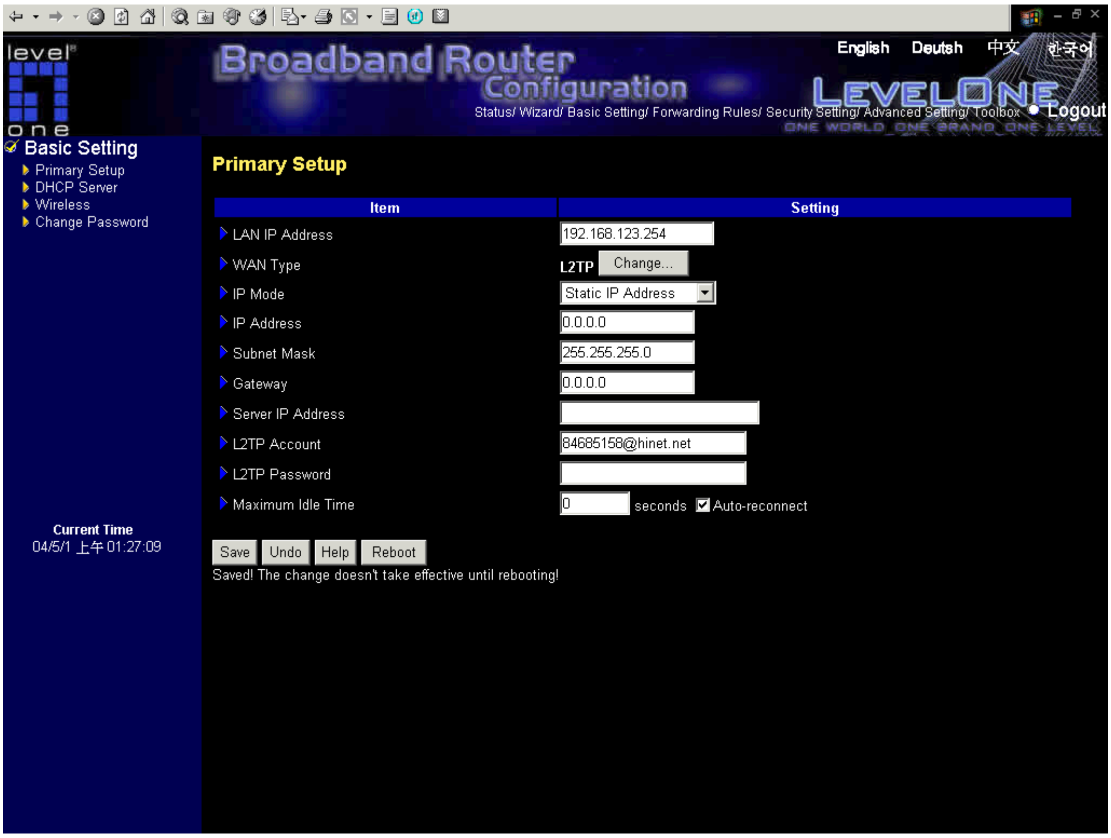
| Item | Setting |
|---|---|
| LAN IP Address | 192.168.123.254 |
| WAN Type | PPTP Change... |
| IP Mode | Static IP Address |
| My IP Address | 0.0.0.0 |
| My Subnet Mask | 255.255.255.0 |
| My Gateway IP | 0.0.0.0 |
| Server IP Address | |
| PPTP Account | 84685158@hinet.net |
| PPTP Password | |
| Connection ID | (optional) |
| Maximum Idle Time | 0 seconds ☑ Auto-reconnect |

Saved! The change doesn't take effective until rebooting!

### 4.4.1.6 L2TP

1. IP Mode: The IP Mode assigned by your ISP. You can select either Static IP Address or Dynamic IP address.
2. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you when your IP Mode is Static IP Address.
3. Server IP Address: the IP address of the L2TP server.
4. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.

Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will automatically connect to ISP after system is restarted or connection is dropped.



Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Current Time
04/5/1 上午 01:27:09

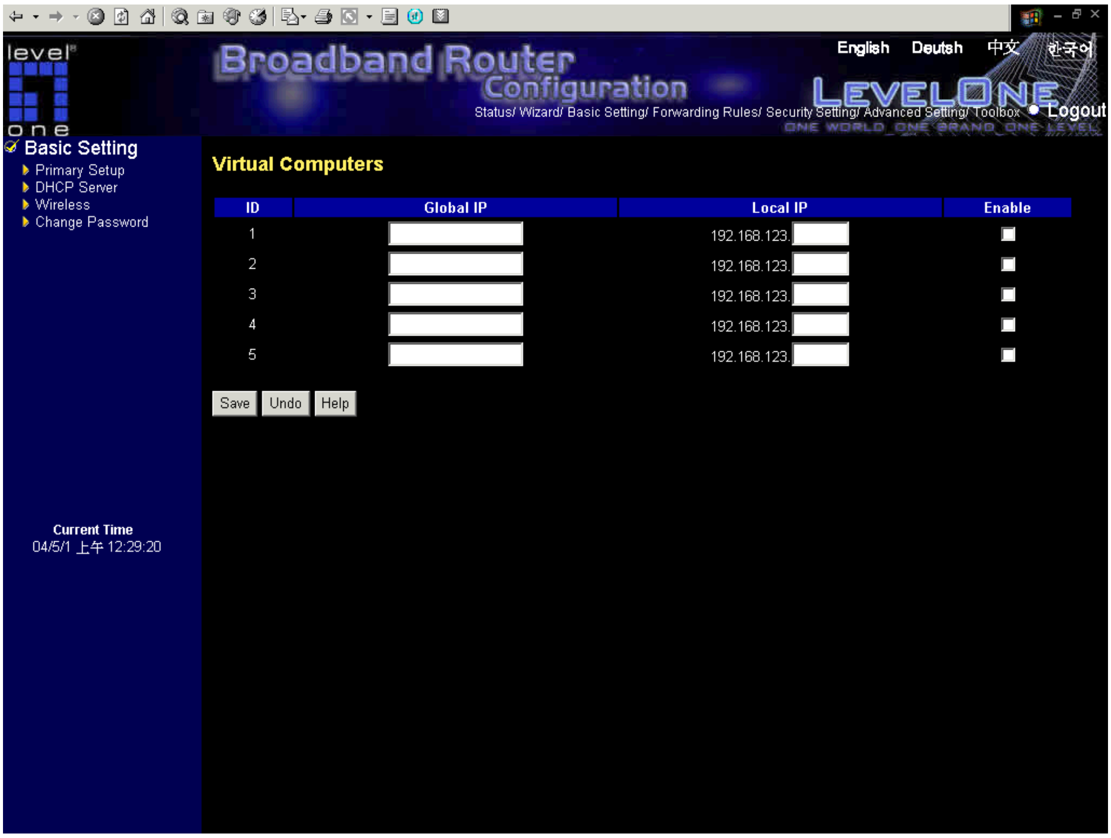
Primary Setup

| Item | Setting |
|---|---|
| LAN IP Address | 192.168.123.254 |
| WAN Type | L2TP Change... |
| IP Mode | Static IP Address |
| IP Address | 0.0.0.0 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 0.0.0.0 |
| Server IP Address | |
| L2TP Account | 84685158@hinet.net |
| L2TP Password | |
| Maximum Idle Time | 0 seconds ☑ Auto-reconnect |

Save Undo Help Reboot

Saved! The change doesn't take effective until rebooting!

### 4.4.1.7 Virtual Computers


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Current Time
04/5/1 上午 12:29:20
Save
Undo
Help

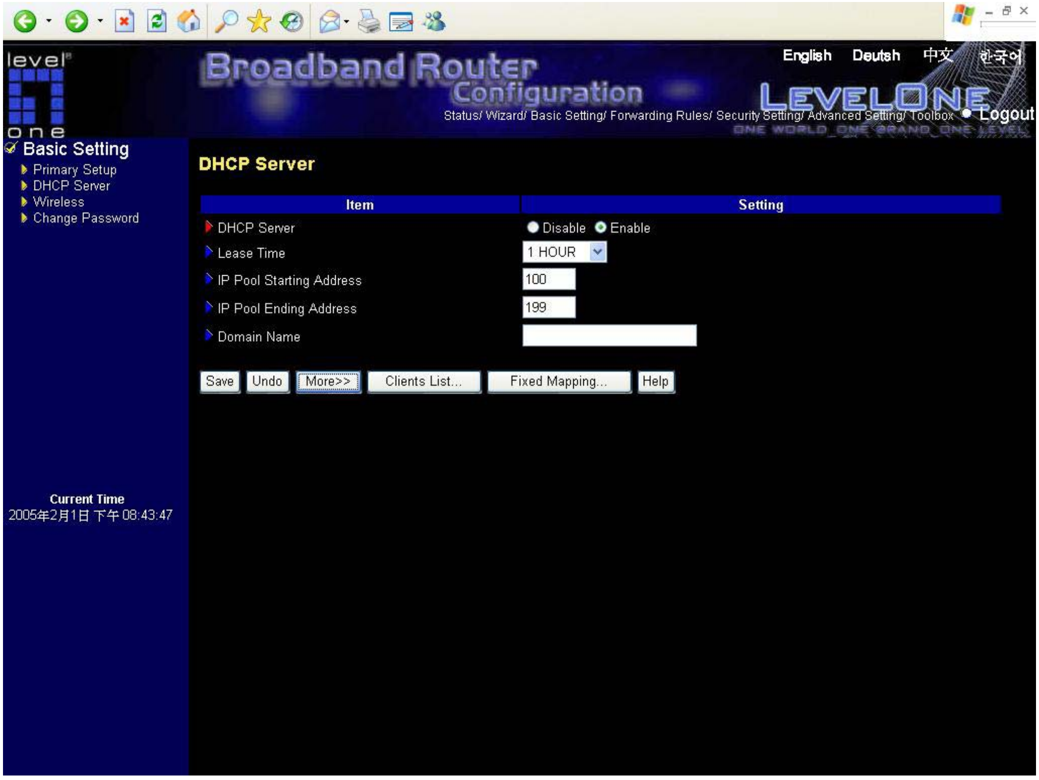
Virtual Computers

| ID | Global IP | Local IP | Enable |
|---|---|---|---|
| 1 |  | 192.168.123. | □ |
| 2 |  | 192.168.123. | □ |
| 3 |  | 192.168.123. | □ |
| 4 |  | 192.168.123. | □ |
| 5 |  | 192.168.123. | □ |

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- Global IP: Enter the global IP address assigned by your ISP.
- Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.
- Enable: Check this item to enable the Virtual Computer feature.

### 4.4.2 DHCP Server

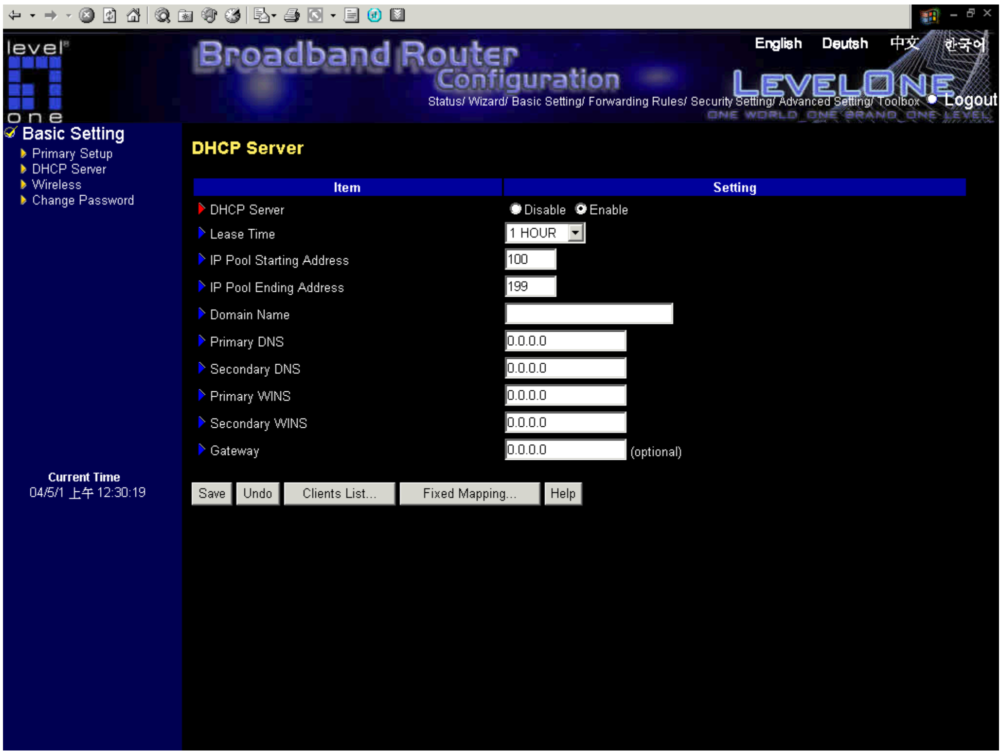

Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
More>>
Clients List...
Fixed Mapping...
Help

DHCP Server

| Item | Setting |
|---|---|
| DHCP Server | ○ Disable ● Enable |
| Lease Time | 1 HOUR |
| IP Pool Starting Address | 100 |
| IP Pool Ending Address | 199 |
| Domain Name | |

Current Time
2005年2月1日 下午 08:43:47

Press **“More>>”**


Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
Clients List...
Fixed Mapping...
Help

DHCP Server

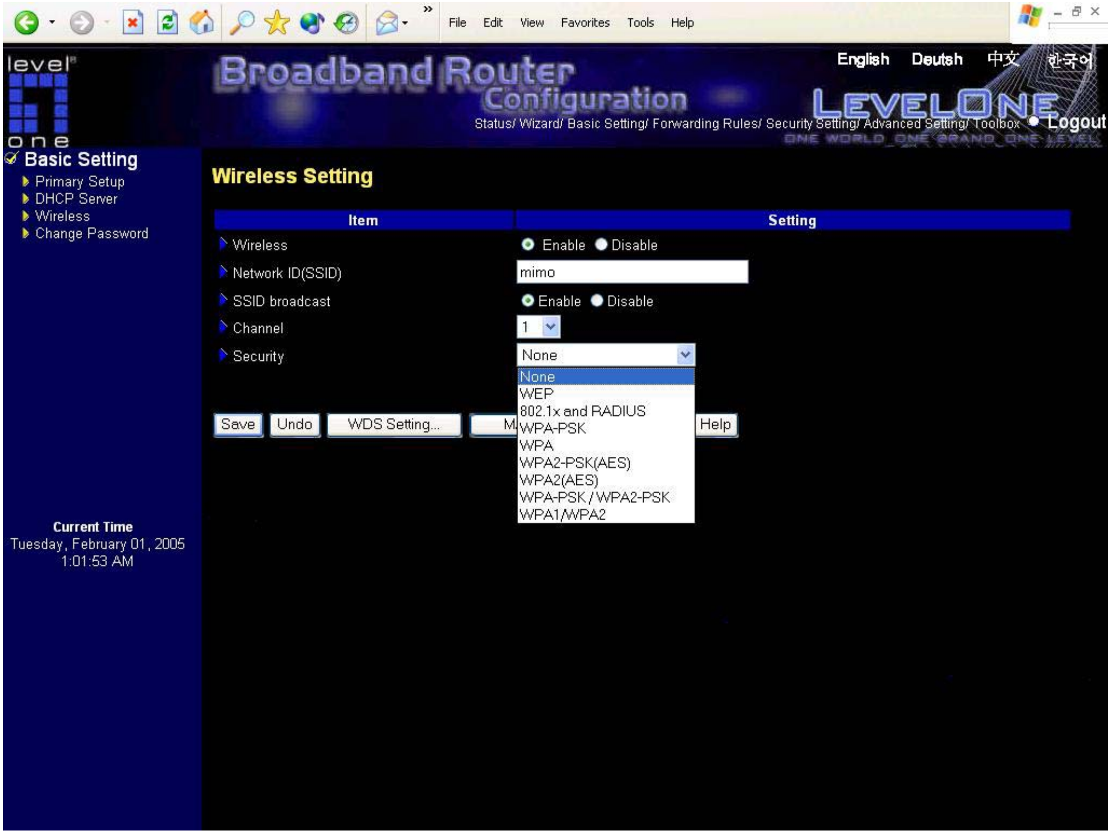
| Item | Setting |
|---|---|
| DHCP Server | ○ Disable ● Enable |
| Lease Time | 1 HOUR |
| IP Pool Starting Address | 100 |
| IP Pool Ending Address | 199 |
| Domain Name | |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Primary WINS | 0.0.0.0 |
| Secondary WINS | 0.0.0.0 |
| Gateway | 0.0.0.0 (optional) |

Current Time
04/5/1 上午 12:30:19

The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

1. **DHCP Server**: Choose "Disable" or "Enable."
2. **Lease Time:** this feature allows you to configure IP's lease time (DHCP client).
3. **IP pool starting Address/ IP pool ending Address**: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name**: Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS**: This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS**: This feature allows you to assign WINS Servers
7. **Gateway**: The Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

### 4.4.3 Wireless Setting, and Security



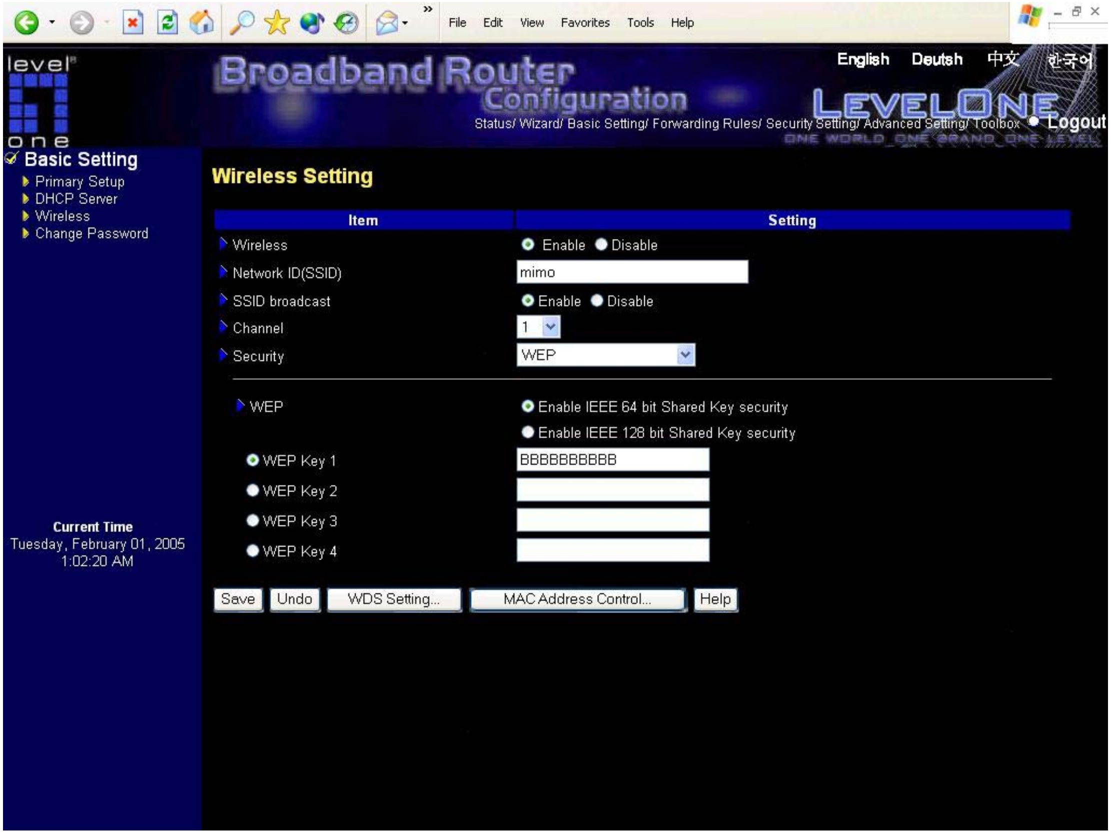
Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | None |

Current Time
Tuesday, February 01, 2005
1:01:53 AM

Wireless settings allow you to set the wireless configuration items.

1. **Wireless function**: Enable or disable wireless function.
2. **Network ID (SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is "**default**")
3. **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is as follow: **channel 11** for North America; **channel 13** for European (ETSI); **channel 14** for Japan.


File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
WDS Setting...
MAC Address Control...
Help

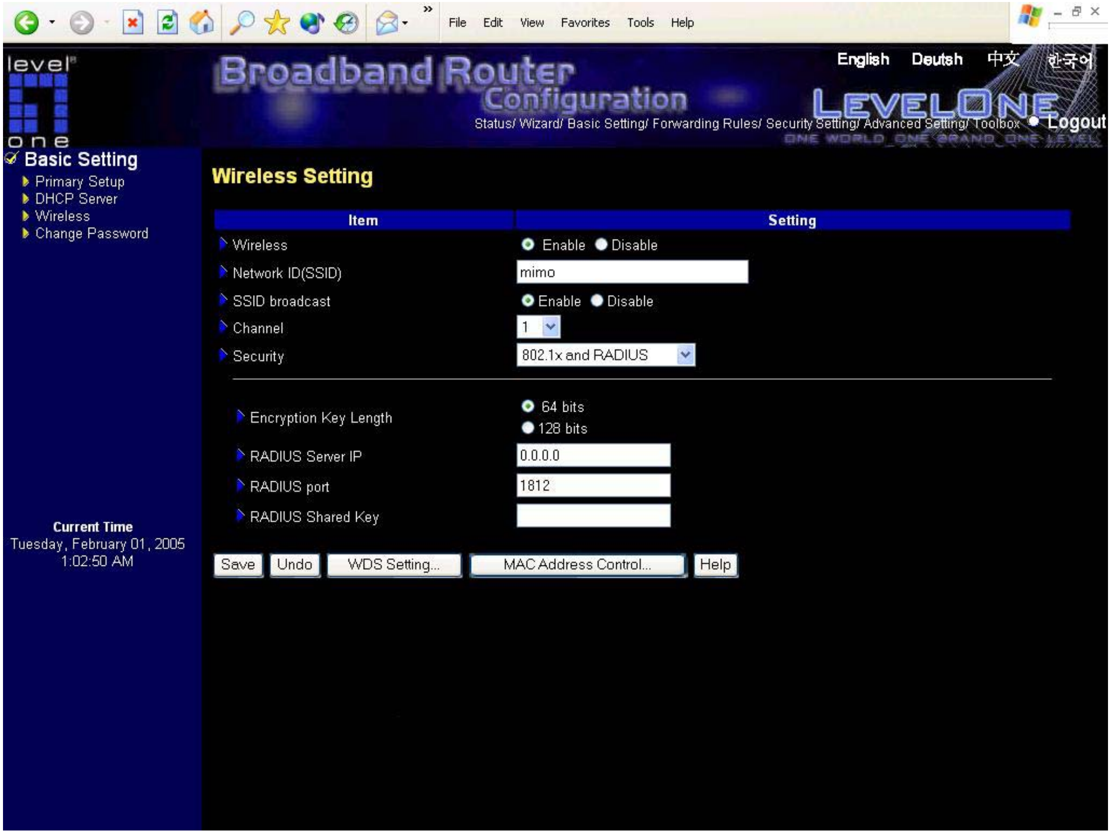
Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WEP |
| WEP | ● Enable IEEE 64 bit Shared Key security<br>○ Enable IEEE 128 bit Shared Key security |
| ● WEP Key 1 | BBBBBBBBBB |
| ○ WEP Key 2 | |
| ○ WEP Key 3 | |
| ○ WEP Key 4 | |

Current Time
Tuesday, February 01, 2005
1:02:20 AM

**WEP Security**: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. The standardized IEEE 802.11 WEP (128 or 64-bit) is used here.

**WEP Key 1, 2, 3 & 4**: When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.



File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
WDS Setting...
MAC Address Control...
Help

Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | 802.1x and RADIUS |
| Encryption Key Length | ● 64 bits<br>○ 128 bits |
| RADIUS Server IP | 0.0.0.0 |
| RADIUS port | 1812 |
| RADIUS Shared Key | |

Current Time
Tuesday, February 01, 2005
1:02:50 AM

**802.1X Setting**

**802.1X**

Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must **authenticate** to this router first to use the Network service.

RADIUS Server IP

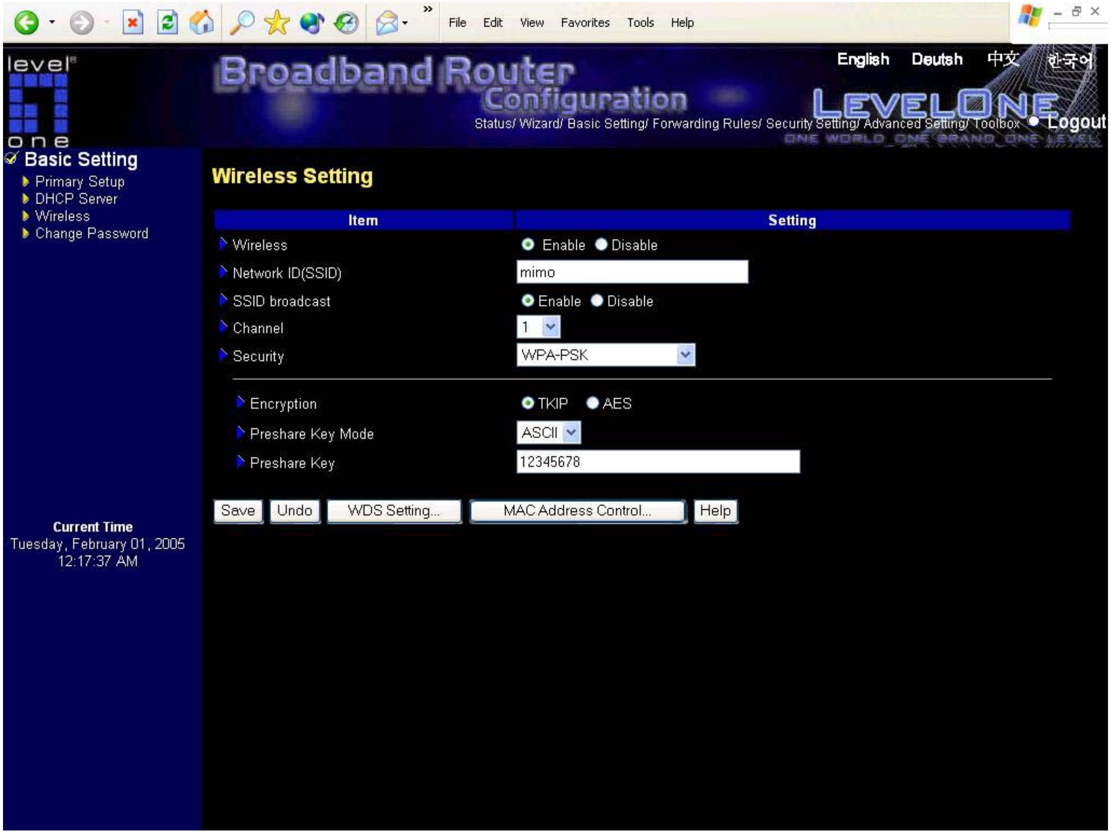
IP address or the 802.1X server's domain-name.

RADIUS port

The port setting of 802.1X server

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.


File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Current Time
Tuesday, February 01, 2005
12:17:37 AM
Save
Undo
WDS Setting...
MAC Address Control...
Help

Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA-PSK |
| Encryption | ● TKIP ○ AES |
| Preshare Key Mode | ASCII |
| Preshare Key | 12345678 |

**WPA-PSK**

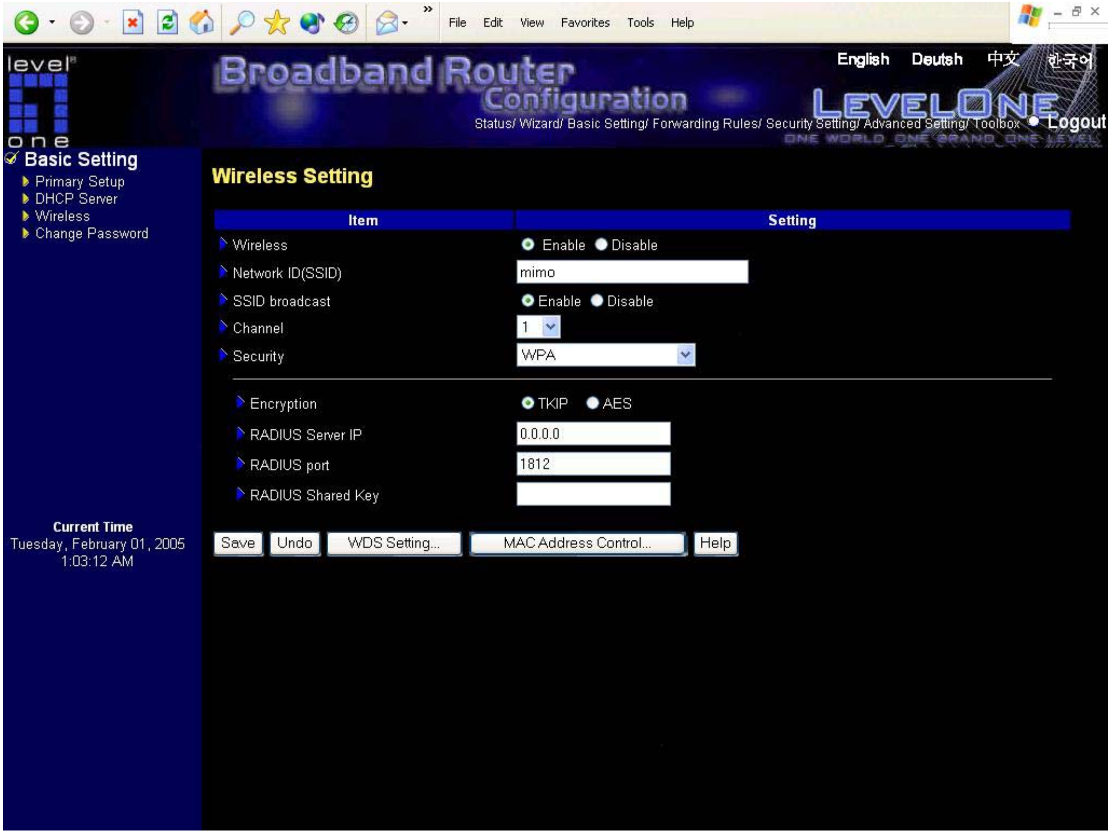
1.Encryption. There are two encryption methods, TKIP and AES.

1. Select Preshare Key Mode

2. Fill in the key, Ex 12345678

**Pre-share Key Mode:** Either ASCII or HEX can be selected.

**Pre-share Key:** Please input either 32 ASCII characters or 64 Hexadecimal digits as Pre-share key.


File Edit View Favorites Tools Help
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password

Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA |
| Encryption | ● TKIP ○ AES |
| RADIUS Server IP | 0.0.0.0 |
| RADIUS port | 1812 |
| RADIUS Shared Key | |

Save | Undo | WDS Setting... | MAC Address Control... | Help

Current Time
Tuesday, February 01, 2005
1:03:12 AM

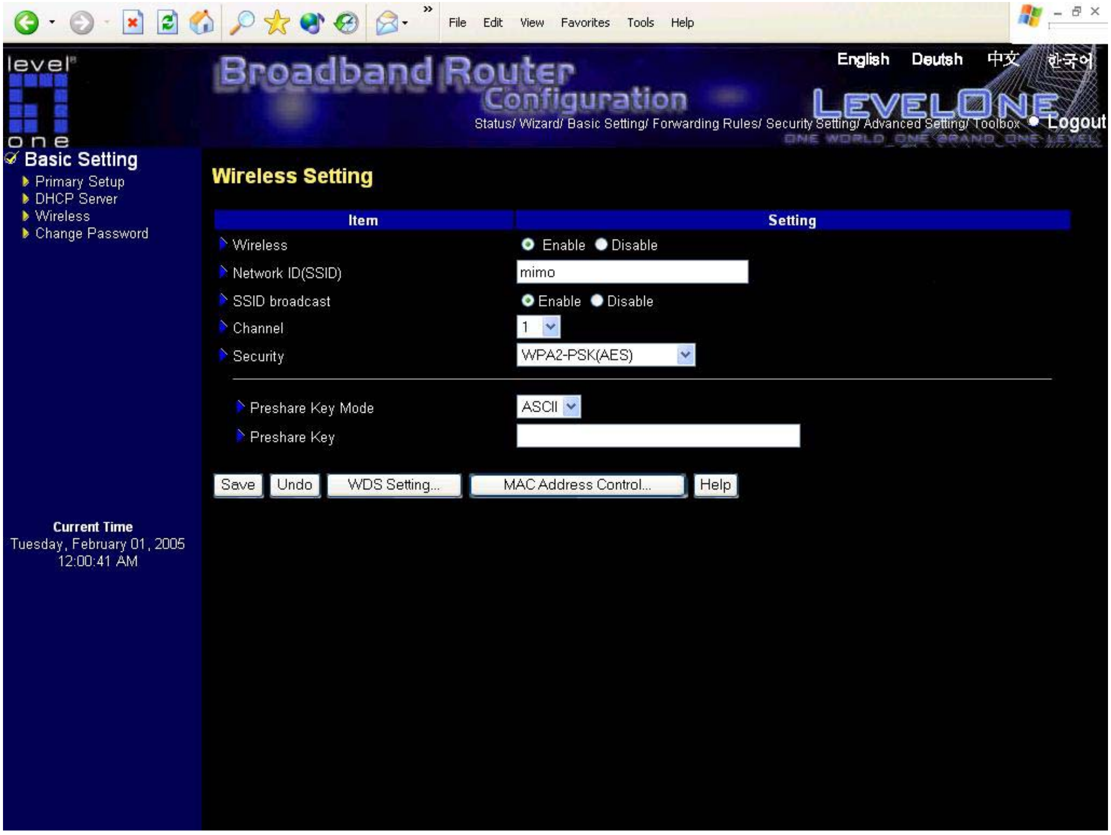
**WPA**

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

IP address or the 802.1X server's domain-name.

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.


File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
WDS Setting...
MAC Address Control...
Help

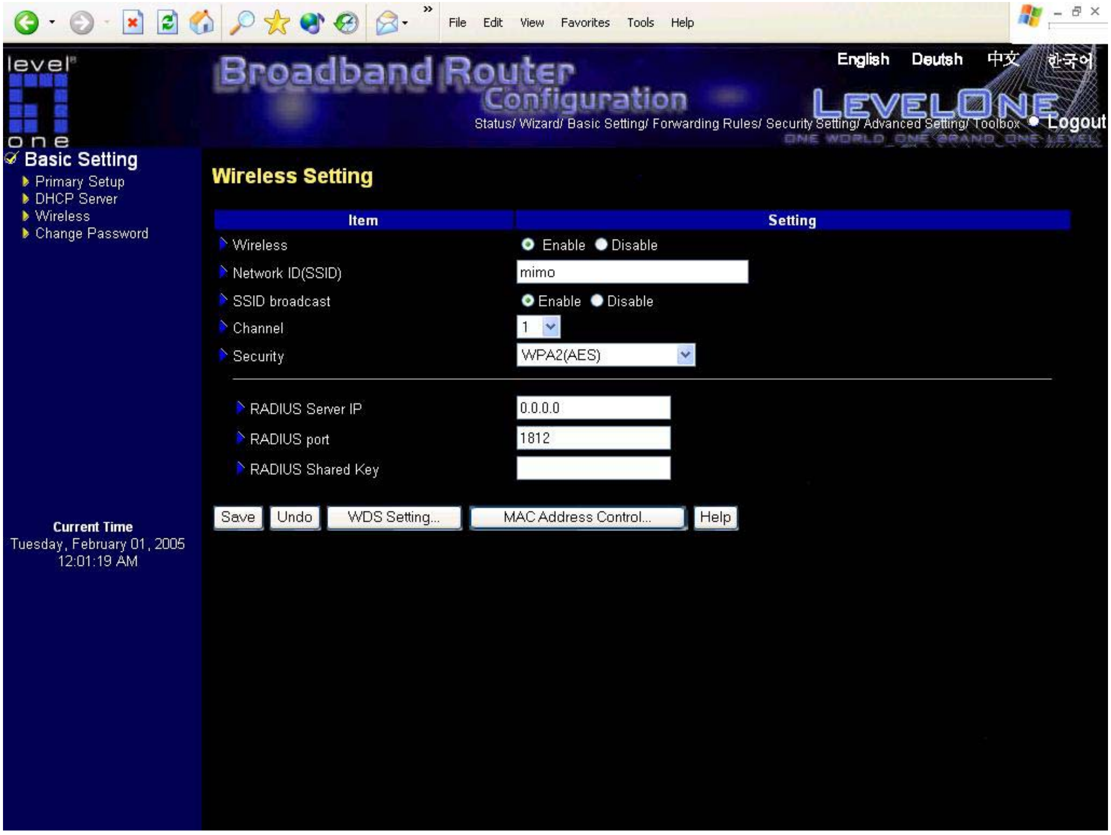
Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA2-PSK(AES) |
| Preshare Key Mode | ASCII |
| Preshare Key | |

Current Time
Tuesday, February 01, 2005
12:00:41 AM

**WPA2-PSK(AES) :** Accept WPA2 clients only and Pre-share key (encryption key) must be entered manually. You can input either 32 ASCII characters or 64 Hexadecimal digits as Pre-share key.

- **Pre-share Key Mode:** Either ASCII or HEX can be selected.
- **Pre-share Key:** Please input either 32 ASCII characters or 64 Hexadecimal digits as Pre-share key.

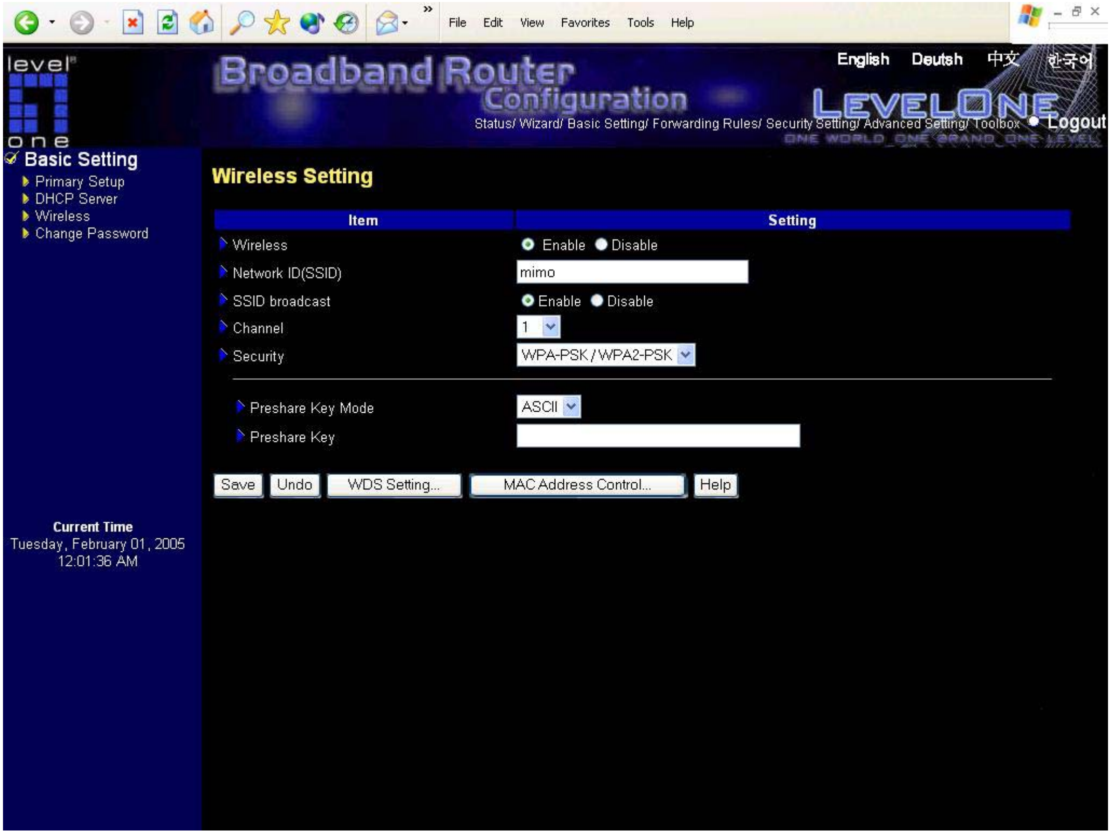

File Edit View Favorites Tools Help
English Deutsh 中文 한국어
level one
Broadband Router Configuration
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Current Time
Tuesday, February 01, 2005
12:01:19 AM
Save
Undo
WDS Setting...
MAC Address Control...
Help

Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA2(AES) |
| RADIUS Server IP | 0.0.0.0 |
| RADIUS port | 1812 |
| RADIUS Shared Key | |

**WPA2(AES) :** Accept WPA2 clients only and work simultaneously with RADIUS Server. The encryption key is got from RADIUS Server dynamically.

- **RADIUS Server IP:** The 802.1X server's IP address.
- **RADIUS port:** The 802.1X server's service port.
- **RADIUS Shared Key:** Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.


File Edit View Favorites Tools Help
level one
Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
WDS Setting...
MAC Address Control...
Help

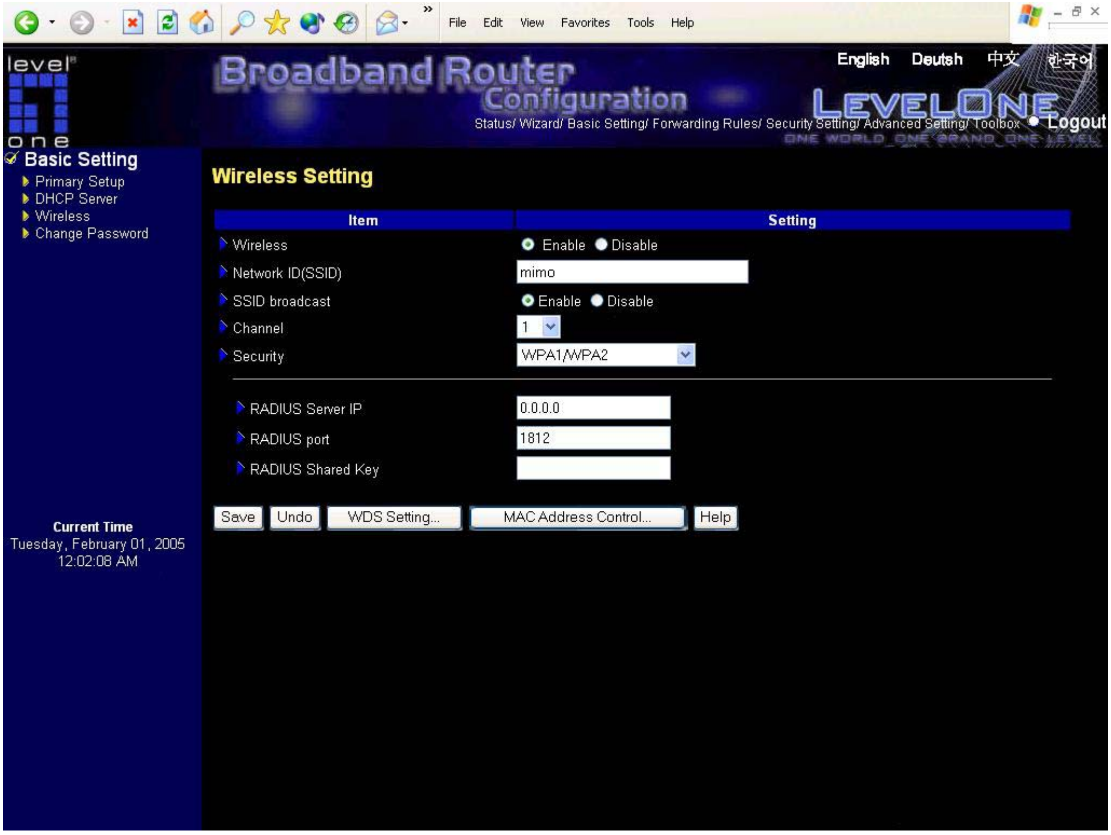
Wireless Setting

| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA-PSK / WPA2-PSK |
| Preshare Key Mode | ASCII |
| Preshare Key | |

Current Time
Tuesday, February 01, 2005
12:01:36 AM

**WPA-PSK / WPA2-PSK :** Accept WPA1 or WPA2 clients to connect simultaneously and Pre-share key (encryption key) must be entered manually. You can input either 32 ASCII characters or 64 Hexadecimal digits as Pre-share key.

- **Pre-share Key Mode:** Either ASCII or HEX can be selected.
- **Pre-share Key:** Please input either 32 ASCII characters or 64 Hexadecimal digits as Pre-share key.


File Edit View Favorites Tools Help
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Basic Setting
Primary Setup
DHCP Server
Wireless
Change Password
Save
Undo
WDS Setting...
MAC Address Control...
Help

Wireless Setting

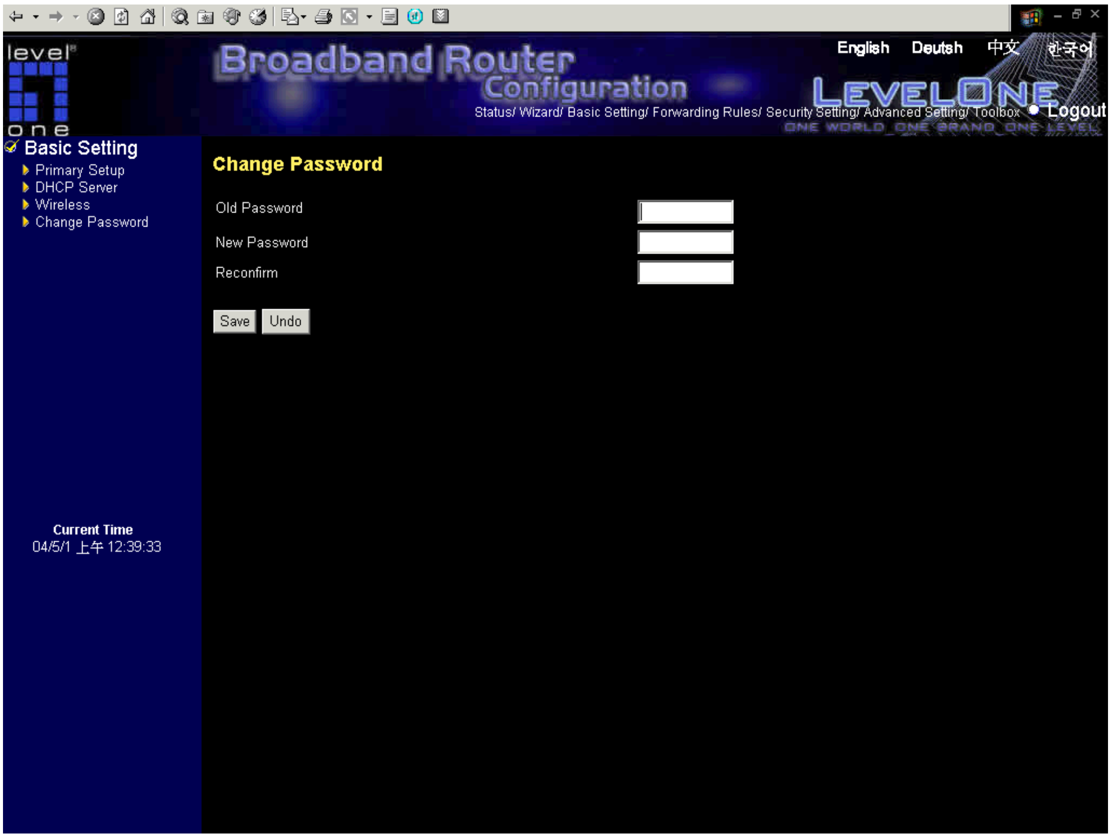
| Item | Setting |
|---|---|
| Wireless | ● Enable ○ Disable |
| Network ID(SSID) | mimo |
| SSID broadcast | ● Enable ○ Disable |
| Channel | 1 |
| Security | WPA1/WPA2 |
| RADIUS Server IP | 0.0.0.0 |
| RADIUS port | 1812 |
| RADIUS Shared Key | |

Current Time
Tuesday, February 01, 2005
12:02:08 AM

**WPA1/WPA2 :** Accept WPA1 or WPA2 clients to connect simultaneously and work simultaneously with RADIUS Server. The encryption key is got from RADIUS Server dynamically.

- **RADIUS Server IP:** The 802.1X server's IP address.
- **RADIUS port:** The 802.1X server's service port.
- **RADIUS Shared Key:** Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

### 4.4.4 Change Password



Change Password

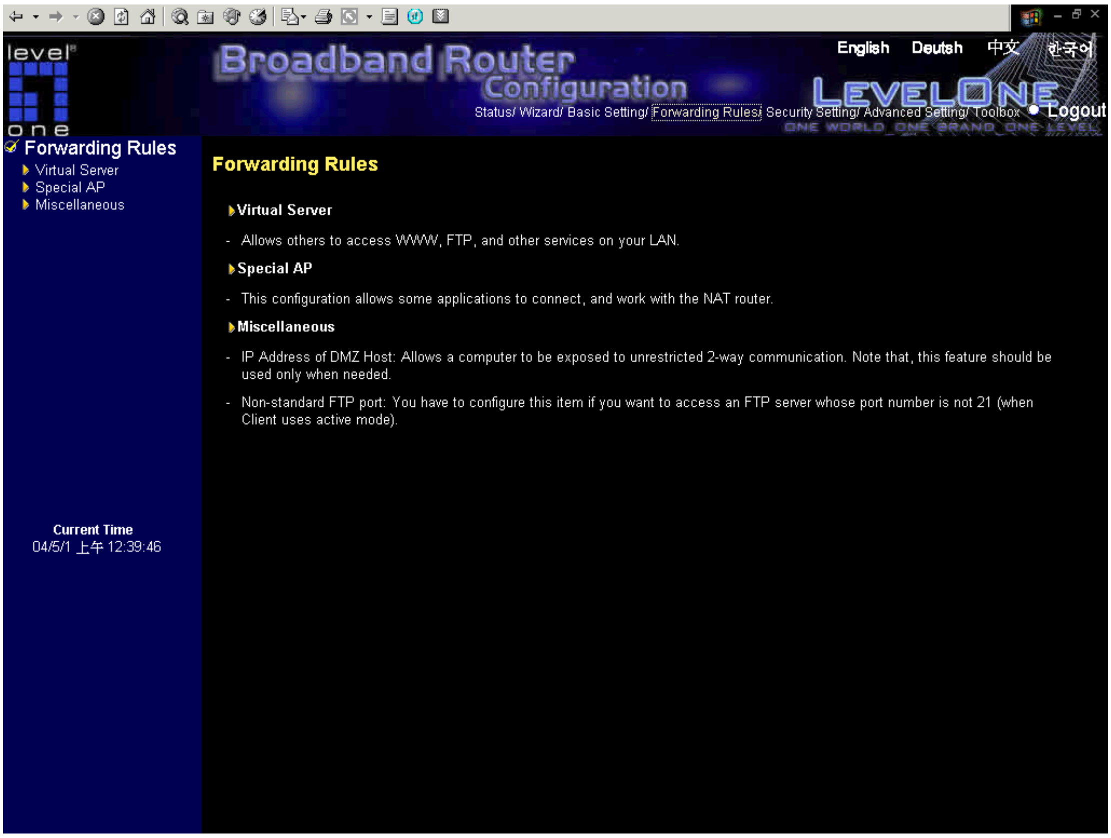
Old Password

New Password

Reconfirm

You can change Password here. We **strongly** recommend you to change the system password for security reason.

## 4.5 Forwarding Rules



Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Forwarding Rules
Virtual Server
Special AP
Miscellaneous
Current Time
04/5/1 上午 12:39:46

Forwarding Rules

**Virtual Server**

- Allows others to access WWW, FTP, and other services on your LAN.

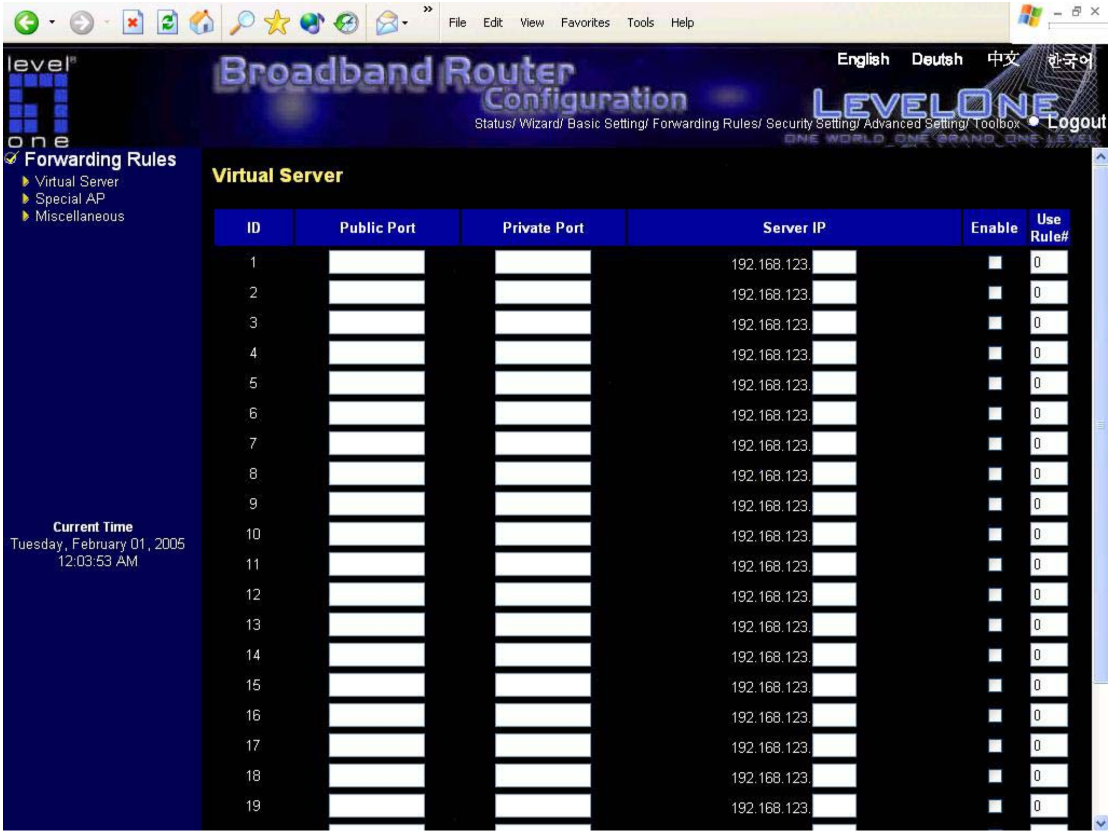
**Special AP**

- This configuration allows some applications to connect, and work with the NAT router.

**Miscellaneous**

- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
- Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).

### 4.5.1 Virtual Server


File
Edit
View
Favorites
Tools
Help
level one
Broadband Router Configuration
English
Deutsh
中文
한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Forwarding Rules
Virtual Server
Special AP
Miscellaneous

Current Time
Tuesday, February 01, 2005
12:03:53 AM

Virtual Server

| ID | Public Port | Private Port | Server IP | Enable | Use Rule# |
|---|---|---|---|---|---|
| 1 | | | 192.168.123. | ☐ | 0 |
| 2 | | | 192.168.123. | ☐ | 0 |
| 3 | | | 192.168.123. | ☐ | 0 |
| 4 | | | 192.168.123. | ☐ | 0 |
| 5 | | | 192.168.123. | ☐ | 0 |
| 6 | | | 192.168.123. | ☐ | 0 |
| 7 | | | 192.168.123. | ☐ | 0 |
| 8 | | | 192.168.123. | ☐ | 0 |
| 9 | | | 192.168.123. | ☐ | 0 |
| 10 | | | 192.168.123. | ☐ | 0 |
| 11 | | | 192.168.123. | ☐ | 0 |
| 12 | | | 192.168.123. | ☐ | 0 |
| 13 | | | 192.168.123. | ☐ | 0 |
| 14 | | | 192.168.123. | ☐ | 0 |
| 15 | | | 192.168.123. | ☐ | 0 |
| 16 | | | 192.168.123. | ☐ | 0 |
| 17 | | | 192.168.123. | ☐ | 0 |
| 18 | | | 192.168.123. | ☐ | 0 |
| 19 | | | 192.168.123. | ☐ | 0 |

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Public Port**, and all requests to this port will be redirected to the **Private Port** of assigned computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

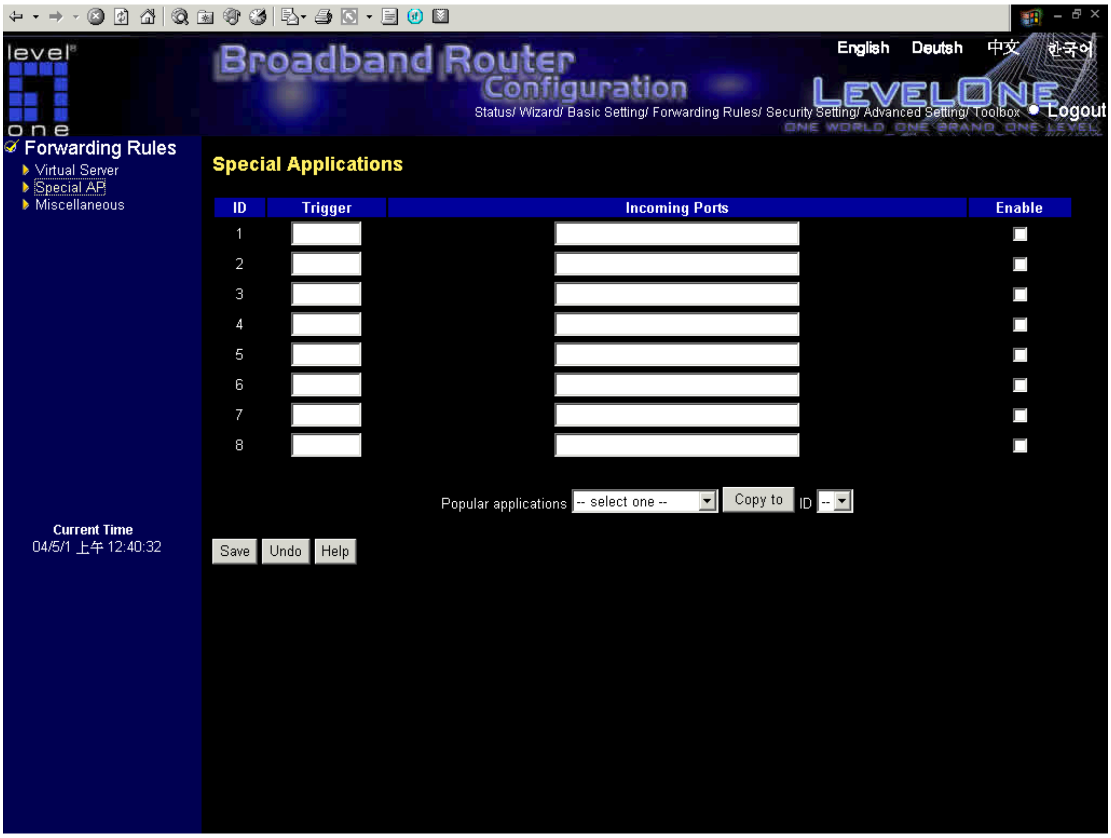
| Public Port | Private | Server IP | Enable |
|---|---|---|---|
| 21 | 21 | 192.168.123.1 | V |
| 80 | 80 | 192.168.123.2 | V |
| 1723 | 1723 | 192.168.123.6 | V |

The Private port is used for multi-computers, which might use the same service.

For example, if you setup three Web server(80) in your LAN, which are 192.168.123.7, 192.168.123.10, and 192.168.123.77. You can assign different public port to different IP. The public port can be set at any port. But please must avoid the confliction. And anyone who would like to connect must be aware of the port difference.

| Public Port | Private | Server IP | Enable |
|---|---|---|---|
| 777 | 80 | 192.168.123.7 | V |
| 888 | 80 | 192.168.123.10 | V |
| 999 | 80 | 192.168.123.77 | V |

## 4.5.2 Special AP


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Forwarding Rules
Virtual Server
Special AP
Miscellaneous

Current Time
04/5/1 上午 12:40:32

Special Applications

| ID | Trigger | Incoming Ports | Enable |
|---|---|---|---|
| 1 | | | ☐ |
| 2 | | | ☐ |
| 3 | | | ☐ |
| 4 | | | ☐ |
| 5 | | | ☐ |
| 6 | | | ☐ |
| 7 | | | ☐ |
| 8 | | | ☐ |

Popular applications -- select one -- Copy to ID --

Save Undo Help

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

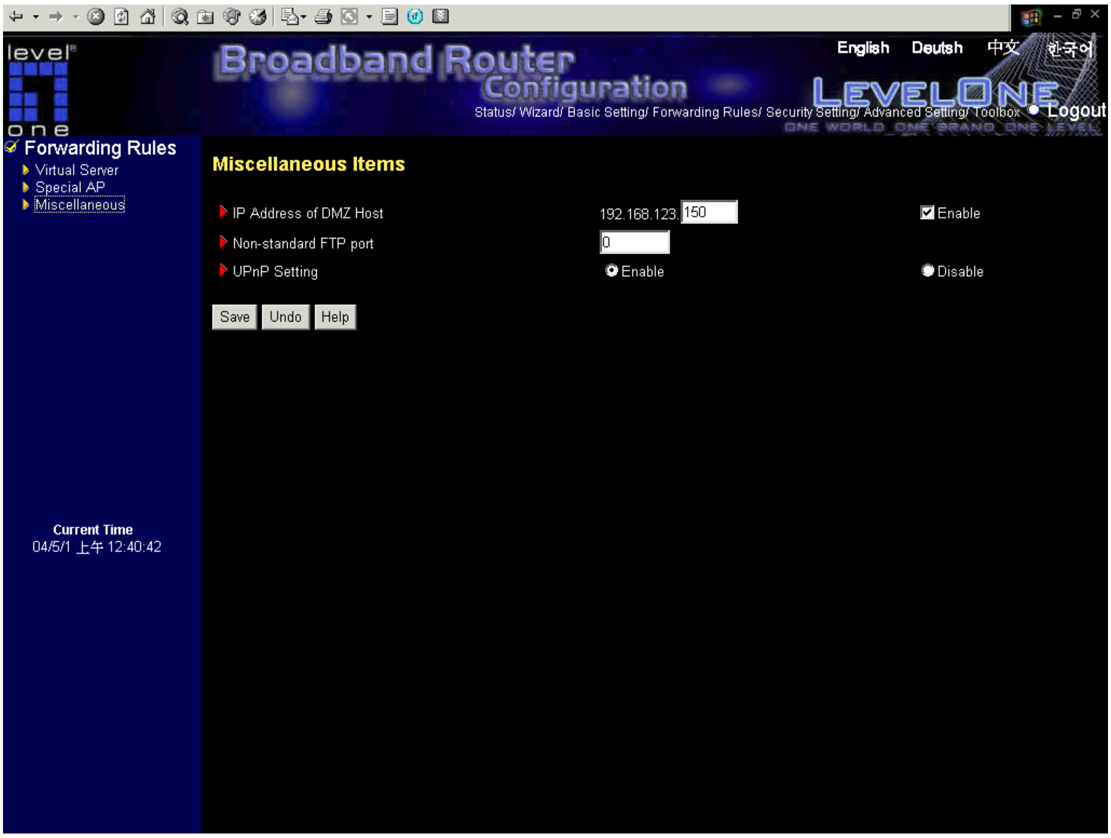
1. **Trigger**: the outbound port number issued by the application..
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

Check **“Enable”** to activate the setting.

### 4.5.3 Miscellaneous Items


level one
Broadband Router Configuration
English
Deutsh
中文
한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Forwarding Rules
Virtual Server
Special AP
Miscellaneous
Current Time
04/5/1 上午 12:40:42
Save
Undo
Help

Miscellaneous Items

IP Address of DMZ Host 192.168.123.150 ☑ Enable

Non-standard FTP port 0

UPnP Setting ● Enable ○ Disable

**IP Address of DMZ Host**

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

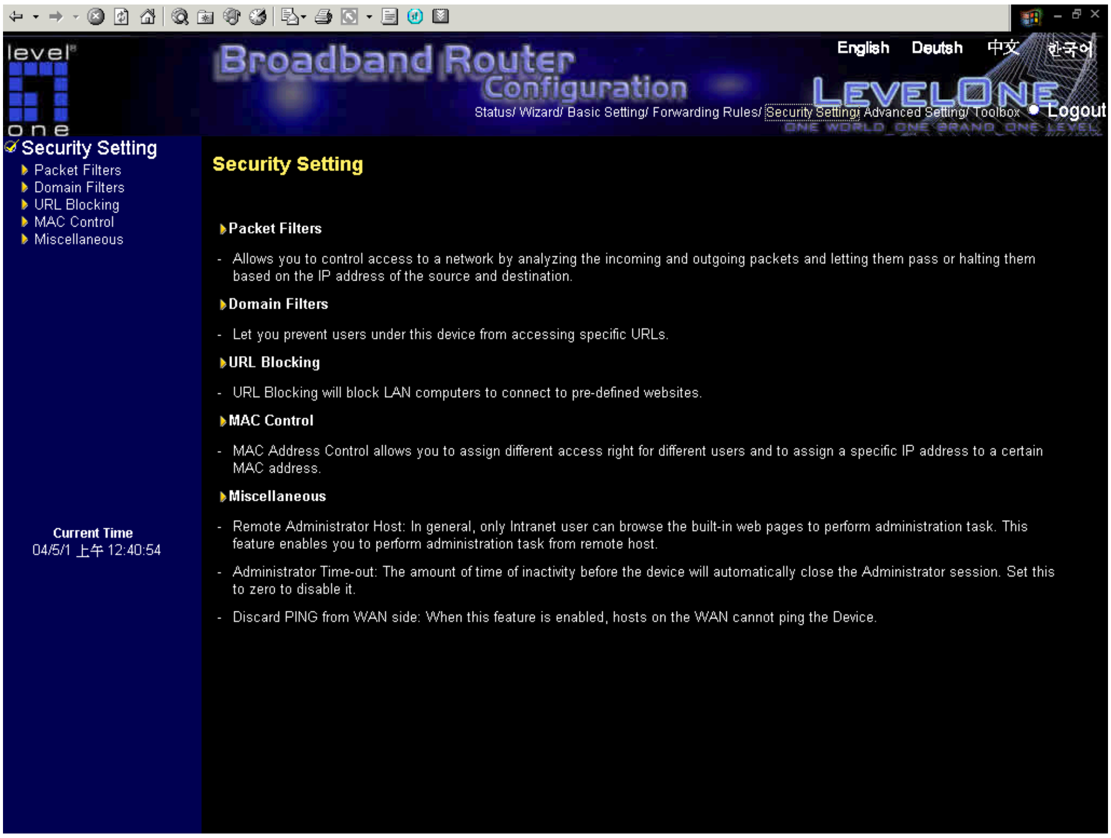
**Non-standard FTP port**

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

**UPnP Setting**

Enable or disable the UPnP function of WBR-5400

## 4.6 Security Settings



Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:40:54

### Security Setting

**Packet Filters**

- Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

**Domain Filters**

- Let you prevent users under this device from accessing specific URLs.

**URL Blocking**

- URL Blocking will block LAN computers to connect to pre-defined websites.

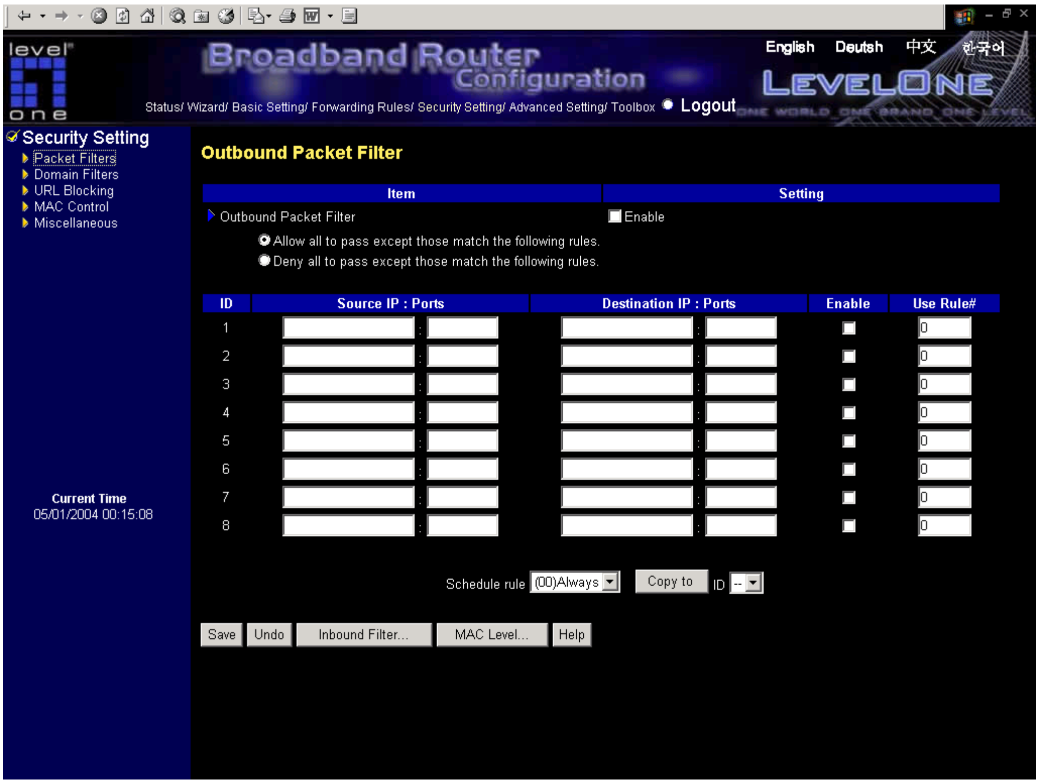
**MAC Control**

- MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

**Miscellaneous**

- Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
- Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
- Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

### 4.6.1 Packet Filter


Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Save
Undo
Inbound Filter...
MAC Level...
Help

Outbound Packet Filter

| Item | Setting |
|---|---|
| Outbound Packet Filter | ☐ Enable |

● Allow all to pass except those match the following rules.

○ Deny all to pass except those match the following rules.

| ID | Source IP : Ports | | Destination IP : Ports | | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 | | | | | ☐ | 0 |
| 2 | | | | | ☐ | 0 |
| 3 | | | | | ☐ | 0 |
| 4 | | | | | ☐ | 0 |
| 5 | | | | | ☐ | 0 |
| 6 | | | | | ☐ | 0 |
| 7 | | | | | ☐ | 0 |
| 8 | | | | | ☐ | 0 |

Schedule rule (00)Always Copy to ID --

Current Time
05/01/2004 00:15:08

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. **Packet Filter** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

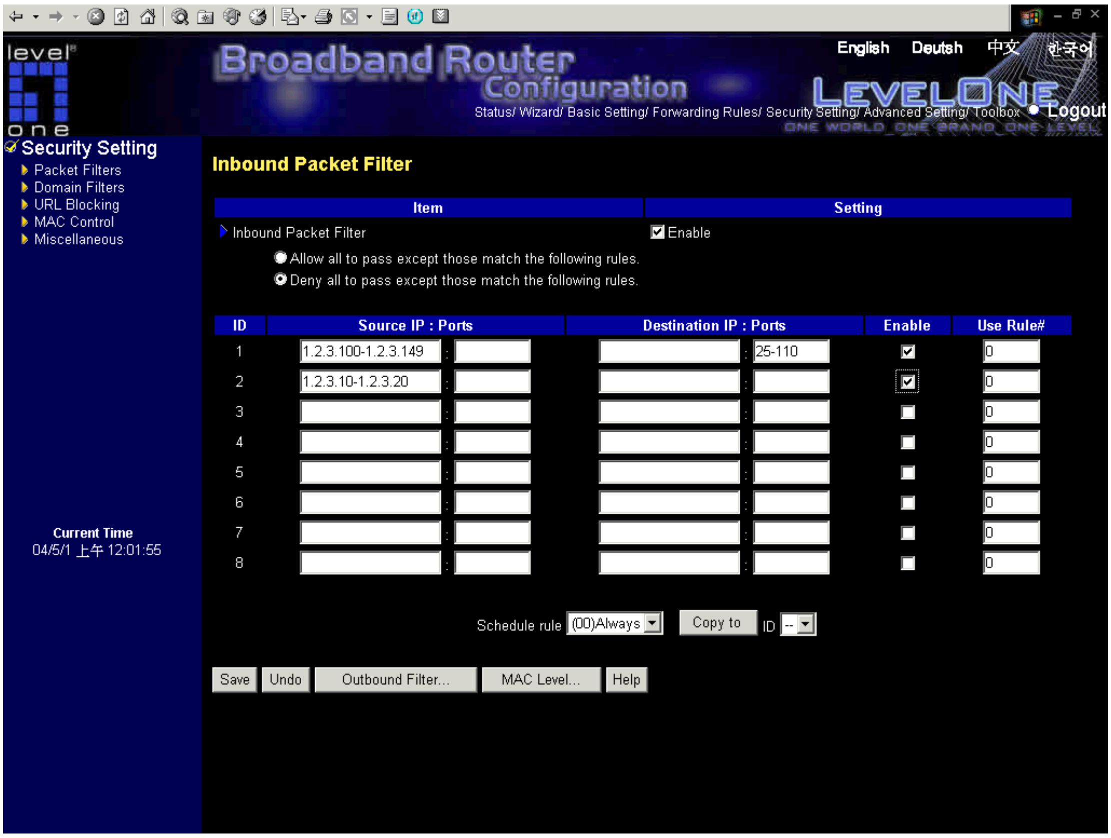
Each rule can be enabled or disabled individually.

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

**Example 1:**


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:01:55

Inbound Packet Filter

| Item | Setting |
|---|---|
| Inbound Packet Filter | ☑ Enable |

○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

| ID | Source IP : Ports | | Destination IP : Ports | | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 | 1.2.3.100-1.2.3.149 | | | 25-110 | ☑ | 0 |
| 2 | 1.2.3.10-1.2.3.20 | | | | ☑ | 0 |
| 3 | | | | | ☐ | 0 |
| 4 | | | | | ☐ | 0 |
| 5 | | | | | ☐ | 0 |
| 6 | | | | | ☐ | 0 |
| 7 | | | | | ☐ | 0 |
| 8 | | | | | ☐ | 0 |

Schedule rule (00)Always [Copy to] ID --

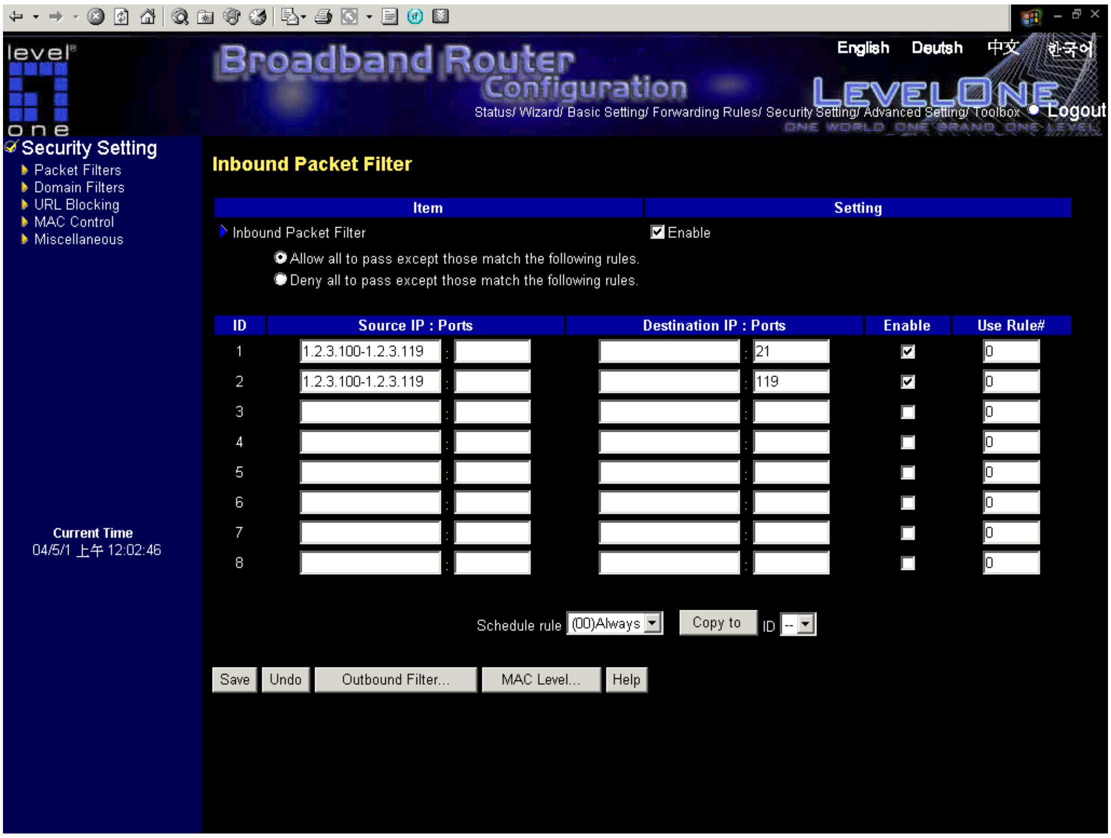
[Save] [Undo] [Outbound Filter...] [MAC Level...] [Help]

(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse your web server as above (port 80)

(1.2.3.10-1.2.3.20) They can do everything (block nothing)

Others are all blocked.

**Example 2:**


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:02:46

Inbound Packet Filter

| Item | Setting |
|---|---|
| Inbound Packet Filter | ☑ Enable |

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

| ID | Source IP : Ports | | Destination IP : Ports | | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 | 1.2.3.100-1.2.3.119 | | | 21 | ☑ | 0 |
| 2 | 1.2.3.100-1.2.3.119 | | | 119 | ☑ | 0 |
| 3 | | | | | □ | 0 |
| 4 | | | | | □ | 0 |
| 5 | | | | | □ | 0 |
| 6 | | | | | □ | 0 |
| 7 | | | | | □ | 0 |
| 8 | | | | | □ | 0 |

Schedule rule (00)Always Copy to ID --

Save
Undo
Outbound Filter...
MAC Level...
Help

(1.2.3.100-1.2.3.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

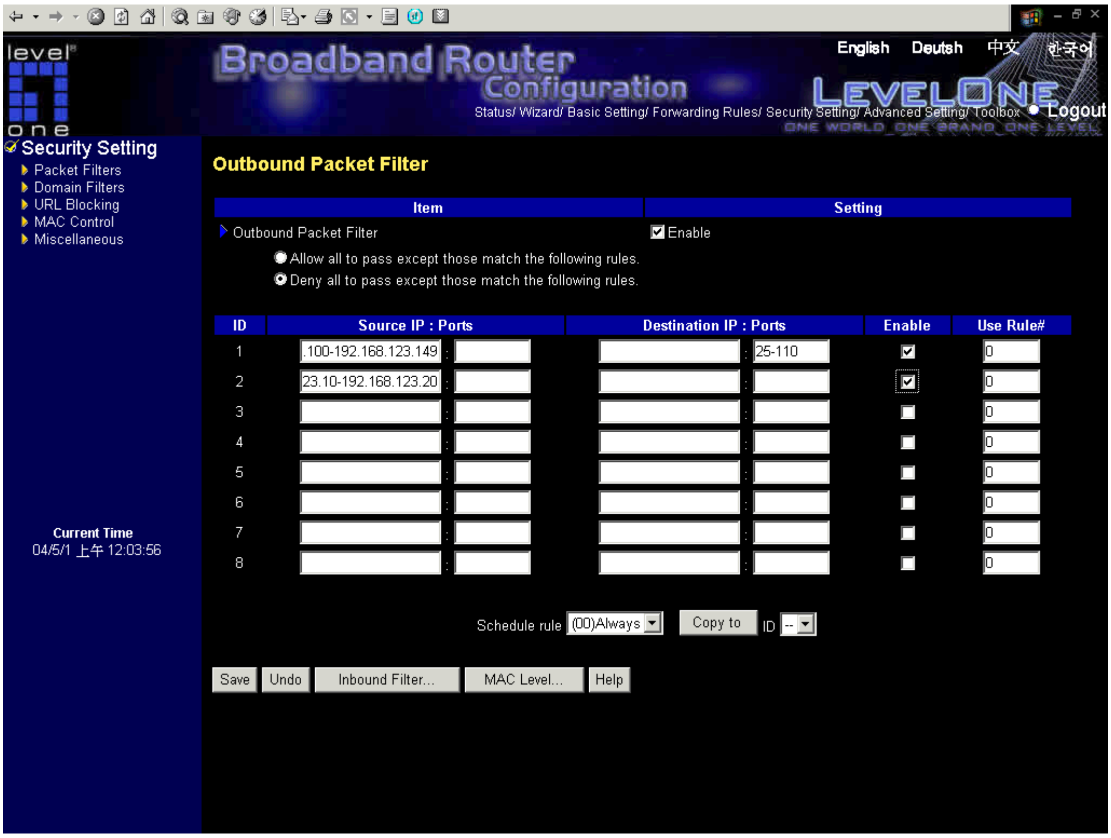
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

**Example 1:**



Broadbband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox ● Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:03:56

**Outbound Packet Filter**

| Item | Setting |
|---|---|
| Outbound Packet Filter | ☑ Enable |

○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

| ID | Source IP | Ports | Destination IP | Ports | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 | .100-192.168.123.149 | | | 25-110 | ☑ | 0 |
| 2 | 23.10-192.168.123.20 | | | | ☑ | 0 |
| 3 | | | | | □ | 0 |
| 4 | | | | | □ | 0 |
| 5 | | | | | □ | 0 |
| 6 | | | | | □ | 0 |
| 7 | | | | | □ | 0 |
| 8 | | | | | □ | 0 |

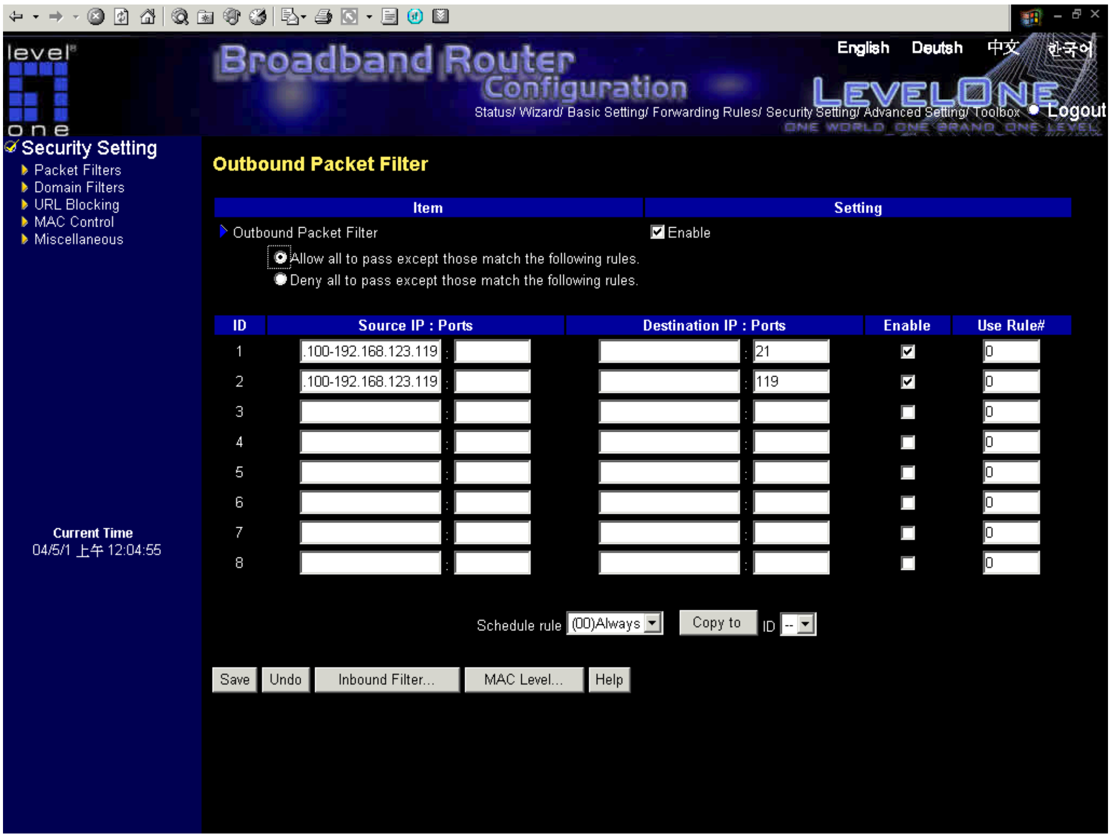
Schedule rule (00)Always Copy to ID --

Save
Undo
Inbound Filter...
MAC Level...
Help

(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)
Others are all blocked.

**Example 2:**


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:04:55
Save
Undo
Inbound Filter...
MAC Level...
Help

Outbound Packet Filter

| Item | Setting |
|---|---|
| Outbound Packet Filter | ☑ Enable |

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

| ID | Source IP : Ports | | Destination IP : Ports | | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 | .100-192.168.123.119 | | | 21 | ☑ | 0 |
| 2 | .100-192.168.123.119 | | | 119 | ☑ | 0 |
| 3 | | | | | ☐ | 0 |
| 4 | | | | | ☐ | 0 |
| 5 | | | | | ☐ | 0 |
| 6 | | | | | ☐ | 0 |
| 7 | | | | | ☐ | 0 |
| 8 | | | | | ☐ | 0 |

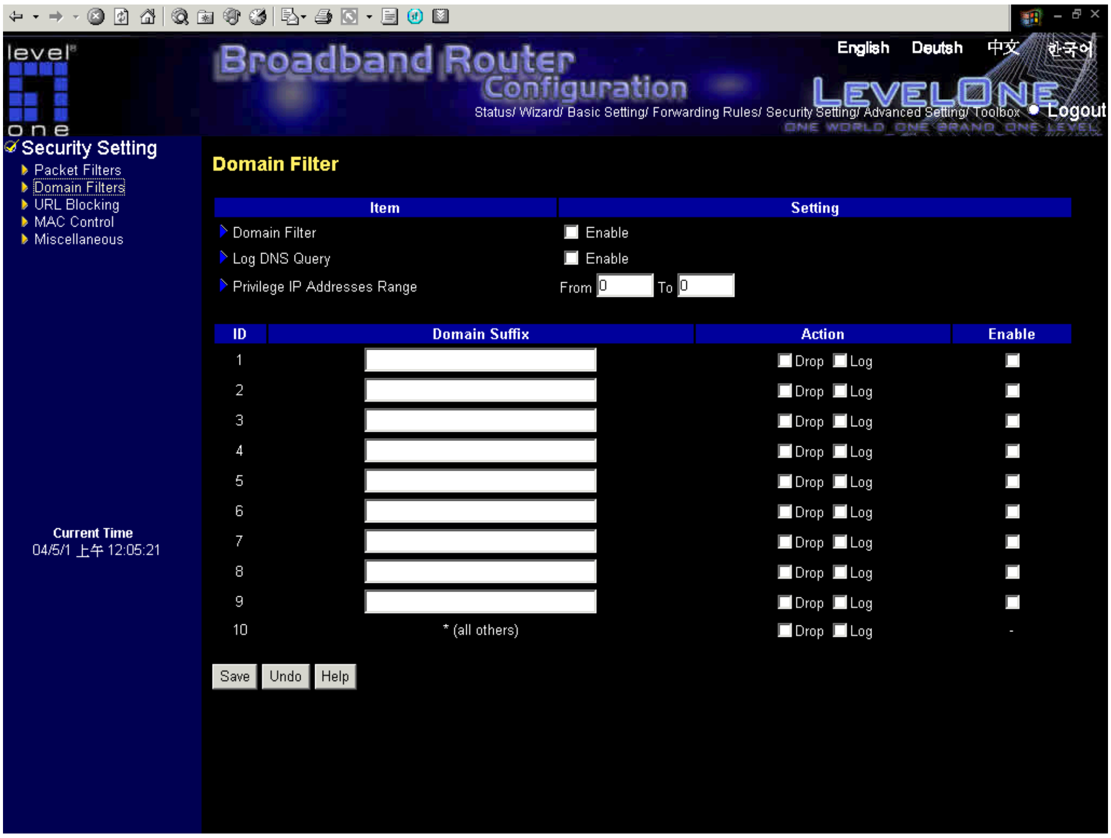
Schedule rule (00)Always Copy to ID --

(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After **Outbound Packet Filter** setting is configured, click the **save** button.

## 4.6.2 Domain Filter



**Domain Filter**

| Item | Setting |
|---|---|
| Domain Filter | □ Enable |
| Log DNS Query | □ Enable |
| Privilege IP Addresses Range | From 0 To 0 |

| ID | Domain Suffix | Action | Enable |
|---|---|---|---|
| 1 | | □ Drop □ Log | □ |
| 2 | | □ Drop □ Log | □ |
| 3 | | □ Drop □ Log | □ |
| 4 | | □ Drop □ Log | □ |
| 5 | | □ Drop □ Log | □ |
| 6 | | □ Drop □ Log | □ |
| 7 | | □ Drop □ Log | □ |
| 8 | | □ Drop □ Log | □ |
| 9 | | □ Drop □ Log | □ |
| 10 | * (all others) | □ Drop □ Log | - |

**Domain Filter**

let you prevent users under this device from accessing specific URLs.

**Domain Filter Enable**

Check if you want to enable Domain Filter.

**Log DNS Query**

Check if you want to log the action when someone accesses the specific URLs.

**Privilege IP Addresses Range**

Setting a group of hosts and privilege these hosts to access network without restriction.

**Domain Suffix**

A suffix of URL to be restricted. For example, ".com", "xxx.com".

**Action**

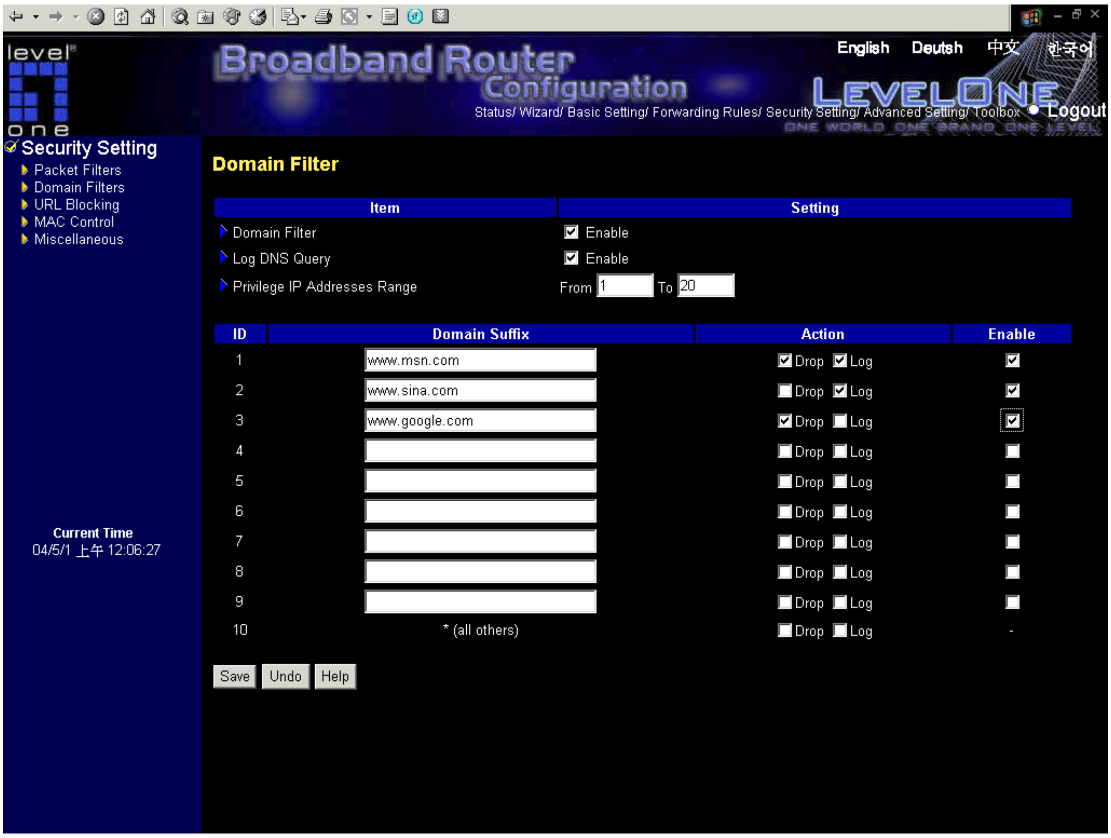
When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check drop to block the access. Check log to log these access.

**Enable**

Check to enable each rule.

**Example:**


level one
Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:06:27
Save
Undo
Help

Domain Filter

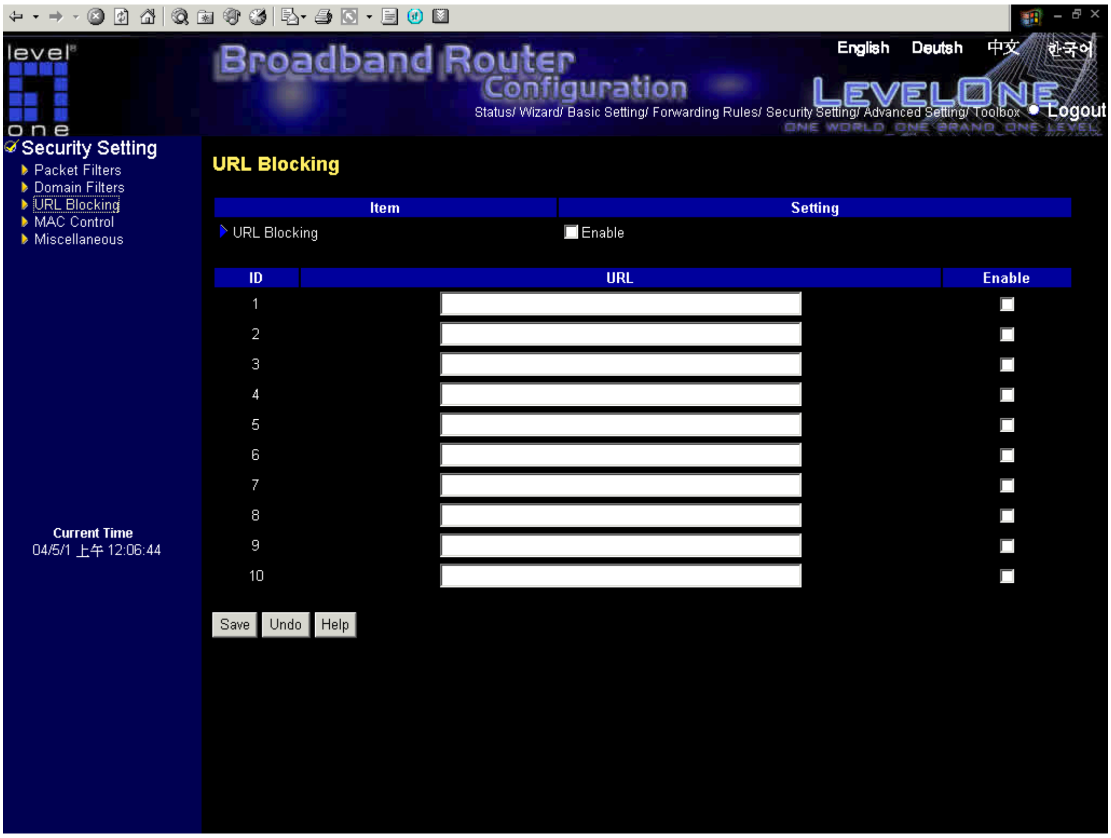
| Item | Setting |
|---|---|
| Domain Filter | ☑ Enable |
| Log DNS Query | ☑ Enable |
| Privilege IP Addresses Range | From 1 To 20 |

| ID | Domain Suffix | Action | Enable |
|---|---|---|---|
| 1 | www.msn.com | ☑ Drop ☑ Log | ☑ |
| 2 | www.sina.com | ☐ Drop ☑ Log | ☑ |
| 3 | www.google.com | ☑ Drop ☐ Log | ☑ |
| 4 | | ☐ Drop ☐ Log | ☐ |
| 5 | | ☐ Drop ☐ Log | ☐ |
| 6 | | ☐ Drop ☐ Log | ☐ |
| 7 | | ☐ Drop ☐ Log | ☐ |
| 8 | | ☐ Drop ☐ Log | ☐ |
| 9 | | ☐ Drop ☐ Log | ☐ |
| 10 | * (all others) | ☐ Drop ☐ Log | - |

In this example:

1. URL include “www.msn.com” will be blocked, and the action will be record in log-file.
2. URL include “www.sina.com” will not be blocked, but the action will be record in log-file.
3. URL include “www.google.com” will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

### 4.6.3 URL Blocking



URL Blocking

| Item | Setting |
|---|---|
| URL Blocking | □ Enable |

| ID | URL | Enable |
|---|---|---|
| 1 | | □ |
| 2 | | □ |
| 3 | | □ |
| 4 | | □ |
| 5 | | □ |
| 6 | | □ |
| 7 | | □ |
| 8 | | □ |
| 9 | | □ |
| 10 | | □ |

**URL Blocking** will block LAN computers to connect to pre-defined Websites.

The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

**URL Blocking Enable**

Checked if you want to enable URL Blocking.

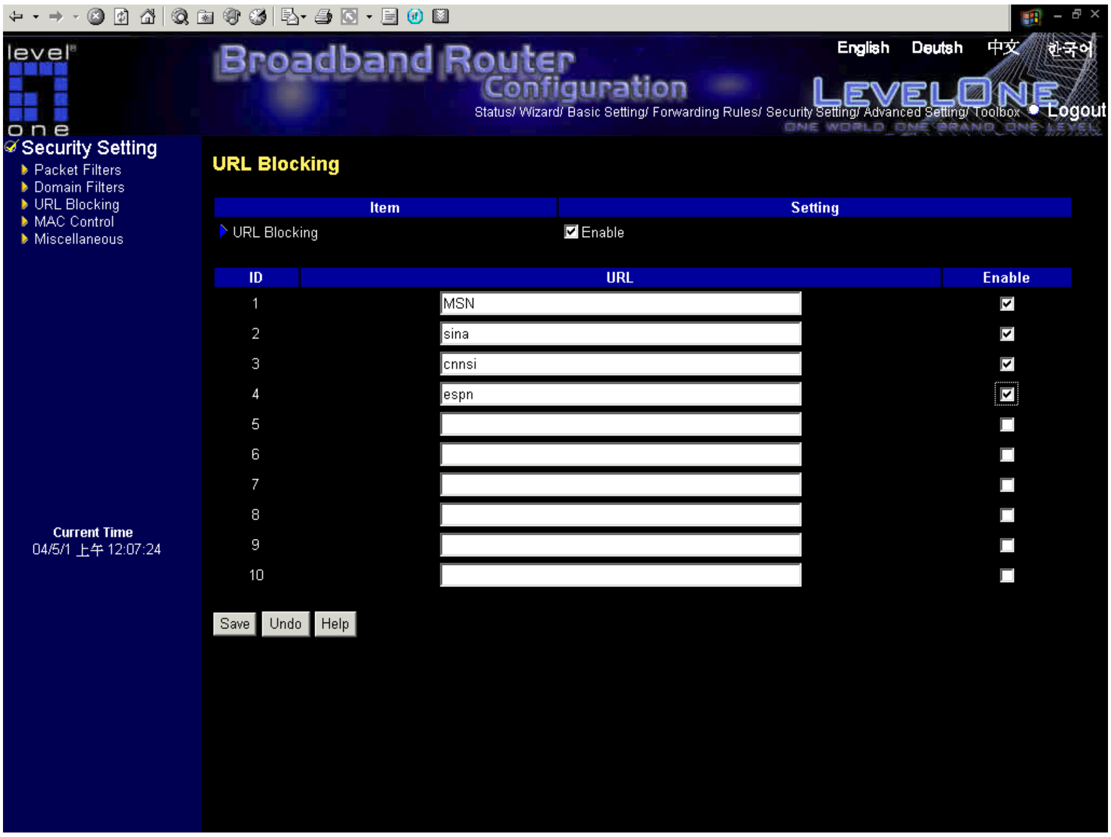
**URL**

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

**Enable**

Checked to enable each rule.



URL Blocking

| Item | Setting |
|---|---|
| URL Blocking | ☑ Enable |

| ID | URL | Enable |
|---|---|---|
| 1 | MSN | ☑ |
| 2 | sina | ☑ |
| 3 | cnnsi | ☑ |
| 4 | espn | ☑ |
| 5 | | □ |
| 6 | | □ |
| 7 | | □ |
| 8 | | □ |
| 9 | | □ |
| 10 | | □ |

In this example:

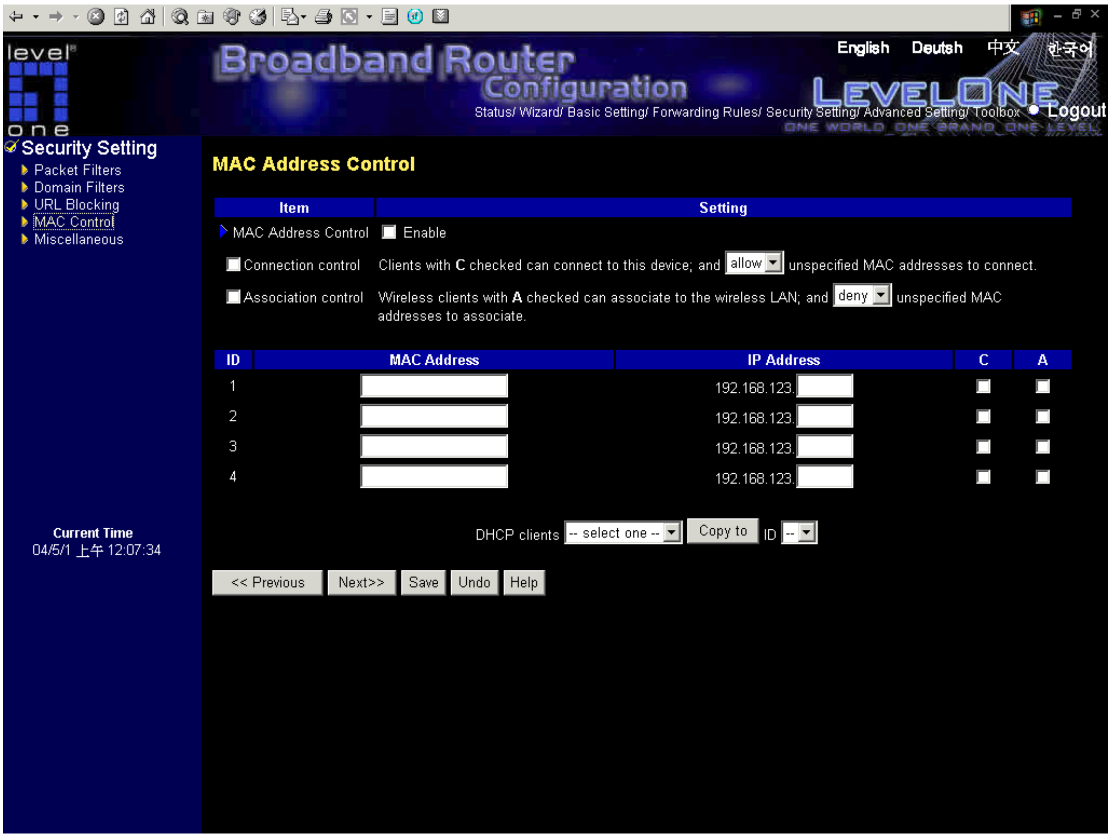
1.URL include “msn” will be blocked, and the action will be record in log-file.

2.URL include “sina” will be blocked, and the action will be record in log-file

3.URL include “cnnsi” will be blocked, and the action will be record in log-file.

4. URL include “espn” will be blocked, and the action will be record in log-file

## 4.6.4 MAC Address Control


Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:07:34

MAC Address Control

| Item | Setting |
|---|---|
| MAC Address Control | □ Enable |
| □ Connection control | Clients with **C** checked can connect to this device; and allow unspecified MAC addresses to connect. |
| □ Association control | Wireless clients with **A** checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate. |

| ID | MAC Address | IP Address | C | A |
|---|---|---|---|---|
| 1 | | 192.168.123. | □ | □ |
| 2 | | 192.168.123. | □ | □ |
| 3 | | 192.168.123. | □ | □ |
| 4 | | 192.168.123. | □ | □ |

DHCP clients -- select one -- Copy to ID --

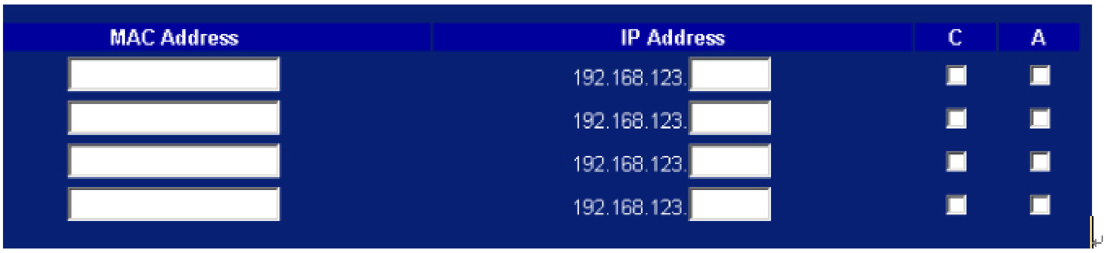
MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

**MAC Address Control** Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

**Connection control** Check "Connection control" to enable the controlling of which wired can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

**Association control** Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

**Control table**

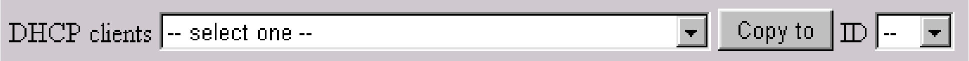


| MAC Address | IP Address | C | A |
|---|---|---|---|
|  | 192.168.123. | □ | □ |
|  | 192.168.123. | □ | □ |
|  | 192.168.123. | □ | □ |
|  | 192.168.123. | □ | □ |

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

|  |  |
|---|---|
| **MAC Address** | MAC address indicates a specific client. |
| **IP Address** | Expected IP address of the corresponding client. Keep it empty if you don't care its IP address. |
| **C** | When "**Connection control**" is checked, check "**C**" will allow the corresponding client to connect to this device. |
| **A** | When "**Association control**" is checked, check "**A**" will allow the corresponding client to associate to the wireless LAN. |

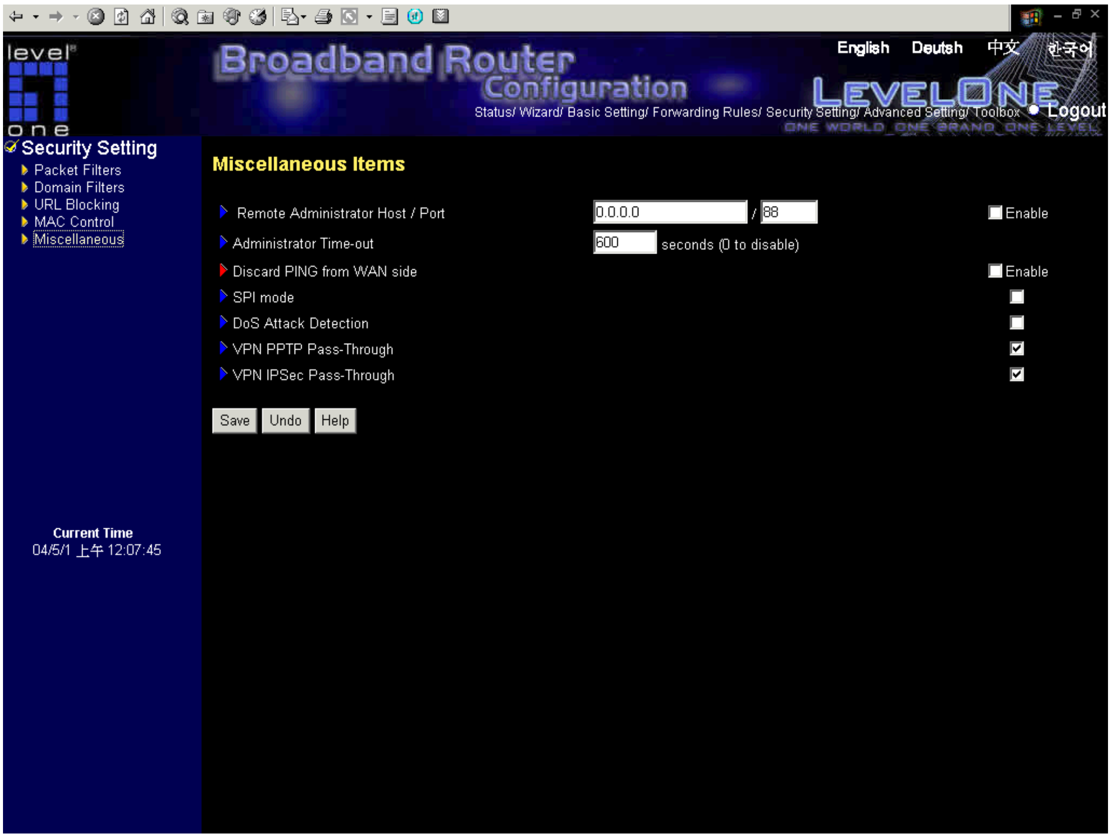
In this page, we provide the following Combobox and button to help you to input the MAC address.



You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

**Previous page and Next Page** To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.

## 4.6.5 Miscellaneous Items


level one
Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Current Time
04/5/1 上午 12:07:45
Save
Undo
Help

Miscellaneous Items

- Remote Administrator Host / Port: 0.0.0.0 / 88 □ Enable
- Administrator Time-out: 600 seconds (0 to disable)
- Discard PING from WAN side: □ Enable
- SPI mode: □
- DoS Attack Detection: □
- VPN PPTP Pass-Through: ☑
- VPN IPSec Pass-Through: ☑

**Remote Administrator Host/Port**

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

**Administrator Time-out**

The time of no activity to logout automatically. Set it to zero to disable this feature.

**Discard PING from WAN side**

When this feature is enabled, any host on the WAN cannot ping this product.

**SPI Mode**

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

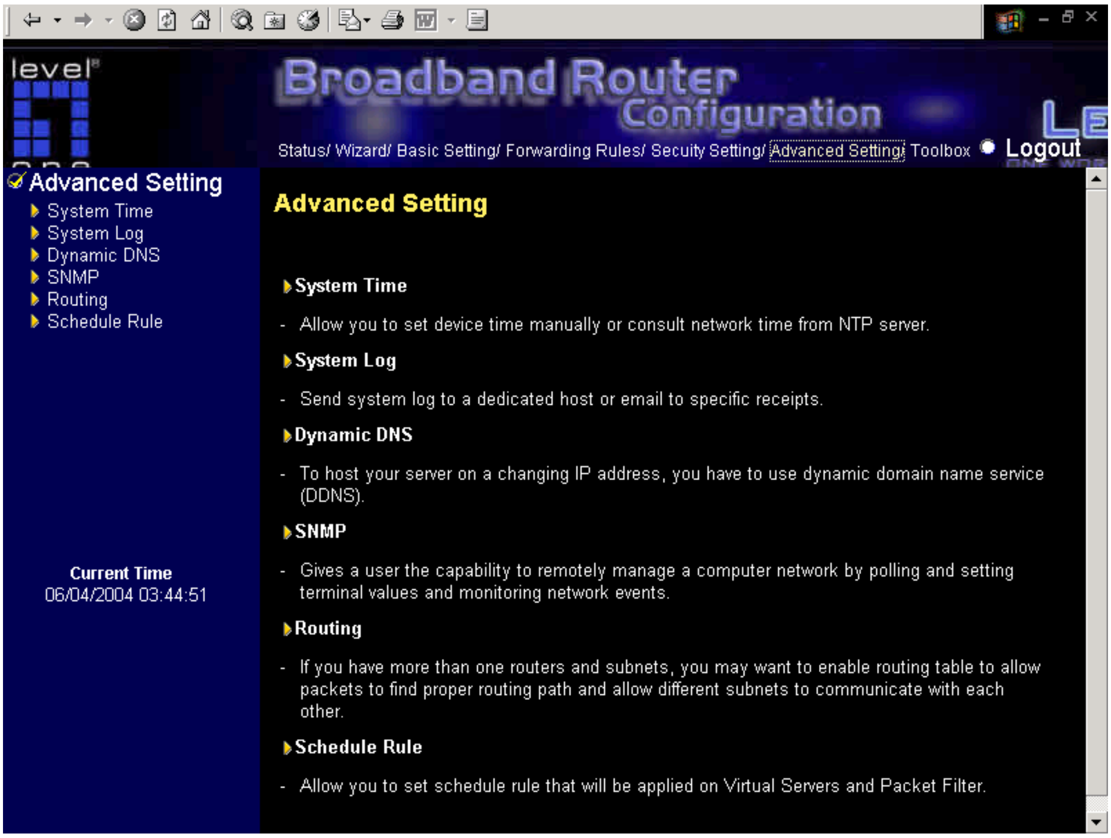
**DoS Attack Detection**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

**VPN PPTP/IPSec Pass-Through**

Please enable this feature, if you need to establish a PPTP or IPSEC connection that will pass through this device.

## 4.7 Advanced Settings


level one
Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout

Advanced Setting
- System Time
- System Log
- Dynamic DNS
- SNMP
- Routing
- Schedule Rule

Current Time
06/04/2004 03:44:51

**Advanced Setting**

**System Time**

- Allow you to set device time manually or consult network time from NTP server.

**System Log**

- Send system log to a dedicated host or email to specific receipts.

**Dynamic DNS**

- To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

**SNMP**

- Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

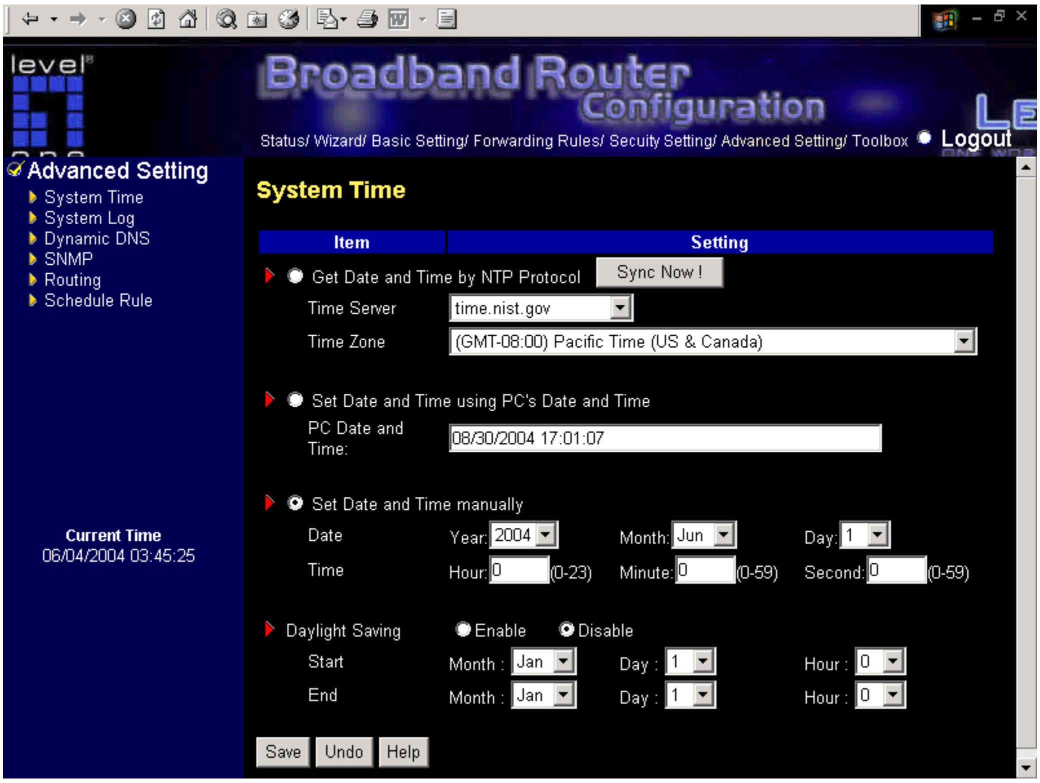
**Routing**

- If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

**Schedule Rule**

- Allow you to set schedule rule that will be applied on Virtual Servers and Packet Filter.

## 4.7.1 System Time


level one
Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Save
Undo
Help

Advanced Setting
- System Time
- System Log
- Dynamic DNS
- SNMP
- Routing
- Schedule Rule

Current Time
06/04/2004 03:45:25

**System Time**

| Item | Setting | | |
|---|---|---|---|
| ○ Get Date and Time by NTP Protocol | Sync Now ! | | |
| Time Server | time.nist.gov | | |
| Time Zone | (GMT-08:00) Pacific Time (US & Canada) | | |
| ○ Set Date and Time using PC's Date and Time | | | |
| PC Date and Time: | 08/30/2004 17:01:07 | | |
| ● Set Date and Time manually | | | |
| Date | Year: 2004 | Month: Jun | Day: 1 |
| Time | Hour: 0 (0-23) | Minute: 0 (0-59) | Second: 0 (0-59) |
| Daylight Saving | ○ Enable | ● Disable | |
| Start | Month : Jan | Day : 1 | Hour : 0 |
| End | Month : Jan | Day : 1 | Hour : 0 |

**Get Date and Time by NTP Protocol**

Selected if you want to Get Date and Time by NTP Protocol.

**Time Server**

Select a NTP time server to consult UTC time

**Time Zone**

Select a time zone where this device locates.

**Get Date and Time using PC`s Date and Time**

Selected if you want to synchronize the router time setting with your connected PC.

**Set Date and Time manually**

Selected if you want to Set Date and Time manually.

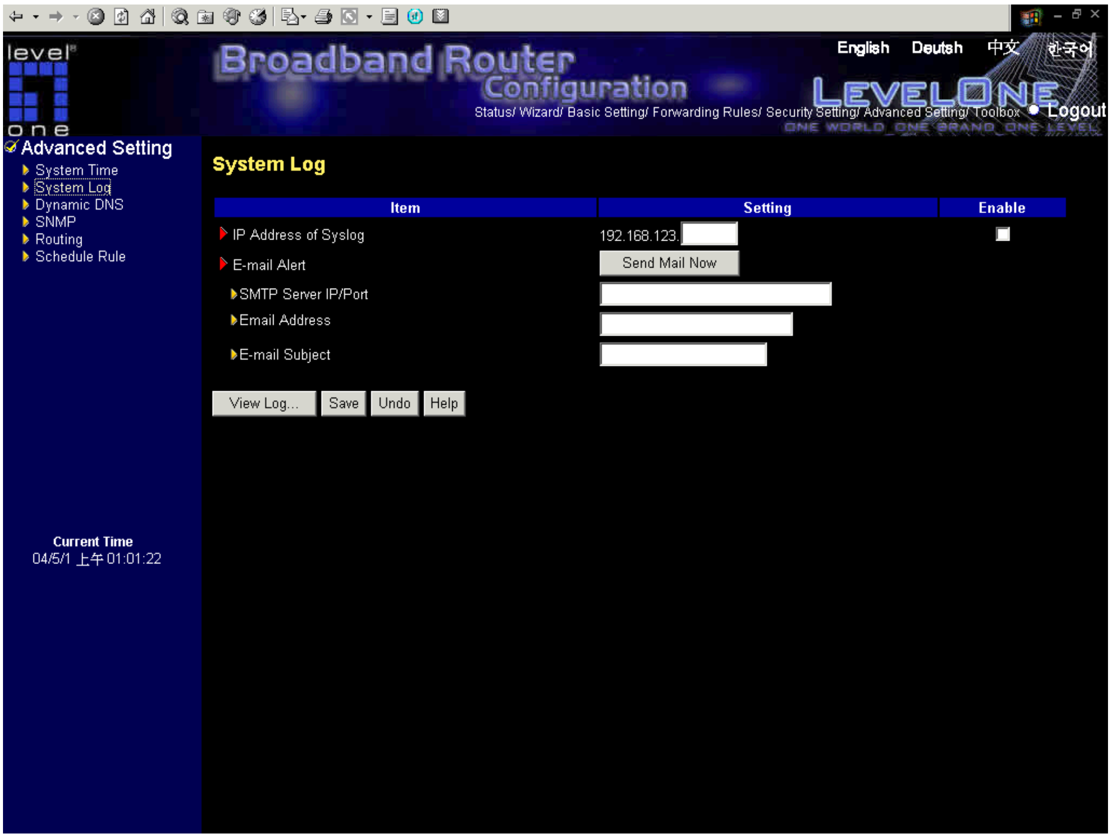
**Daylight Saving**

Select and configure the daylight saving period to fit the local environment.

**Function of Buttons**

**Sync Now:** Synchronize system time with network time server

## 4.7.2 System Log


level one
Broadband Router Configuration
English
Deutsh
中文
한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
View Log...
Save
Undo
Help

System Log

| Item | Setting | Enable |
|---|---|---|
| IP Address of Syslog | 192.168.123. | □ |
| E-mail Alert | Send Mail Now | |
| SMTP Server IP/Port | | |
| Email Address | | |
| E-mail Subject | | |

Current Time
04/5/1 上午 01:01:22

This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

**IP Address for Syslog Server**

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

**E-mail Alert Enable**

Check if you want to enable Email alert(send syslog via email).

**SMTP Server IP/Port**

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

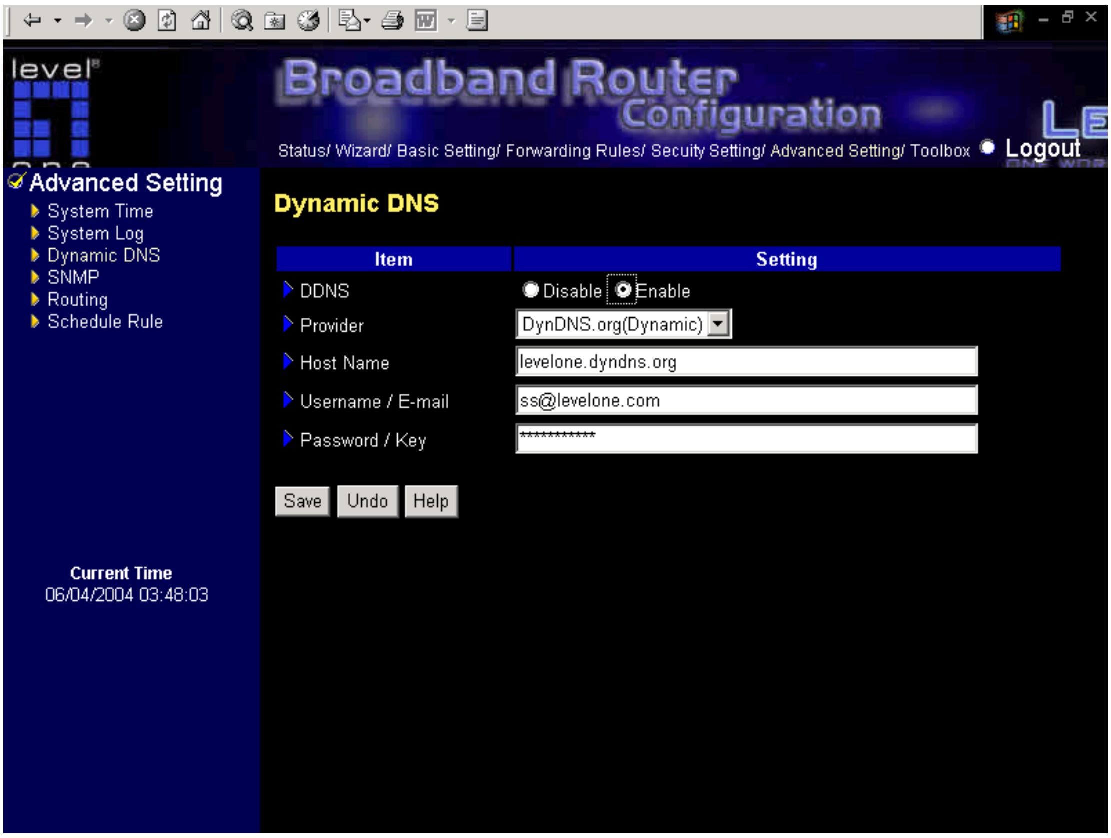
**E-mail addresses**

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

**E-mail Subject**

The subject of email alert. This setting is optional.

### 4.7.3 Dynamic DNS


level one
Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Undo
Help

Current Time
06/04/2004 03:48:03

Dynamic DNS

| Item | Setting |
|---|---|
| DDNS | ○ Disable ● Enable |
| Provider | DynDNS.org(Dynamic) |
| Host Name | levelone.dyndns.org |
| Username / E-mail | ss@levelone.com |
| Password / Key | ************ |

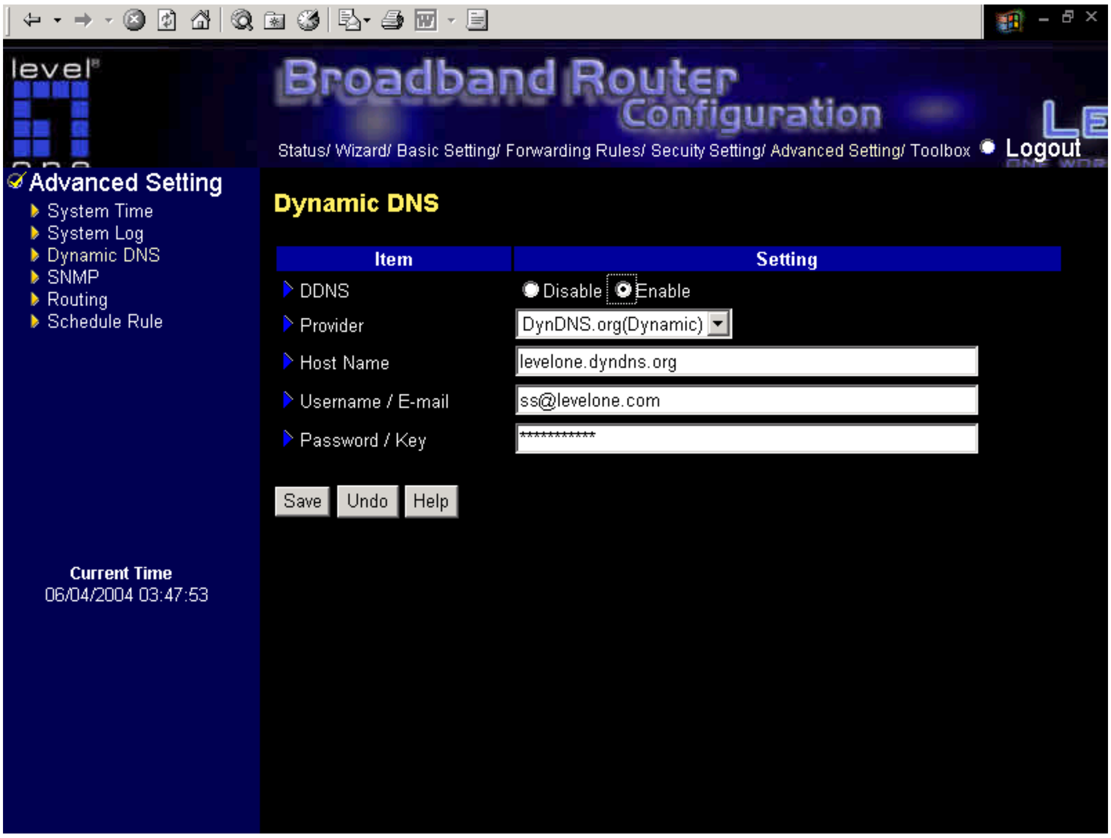
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.
Next you can enter the appropriate information about your Dynamic DNS Server.
You have to define:
Provider
Host Name
Username/E-mail
Password/Key
You will get this information when you register an account on a Dynamic DNS server.

**Example:**


Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Undo
Help

Dynamic DNS

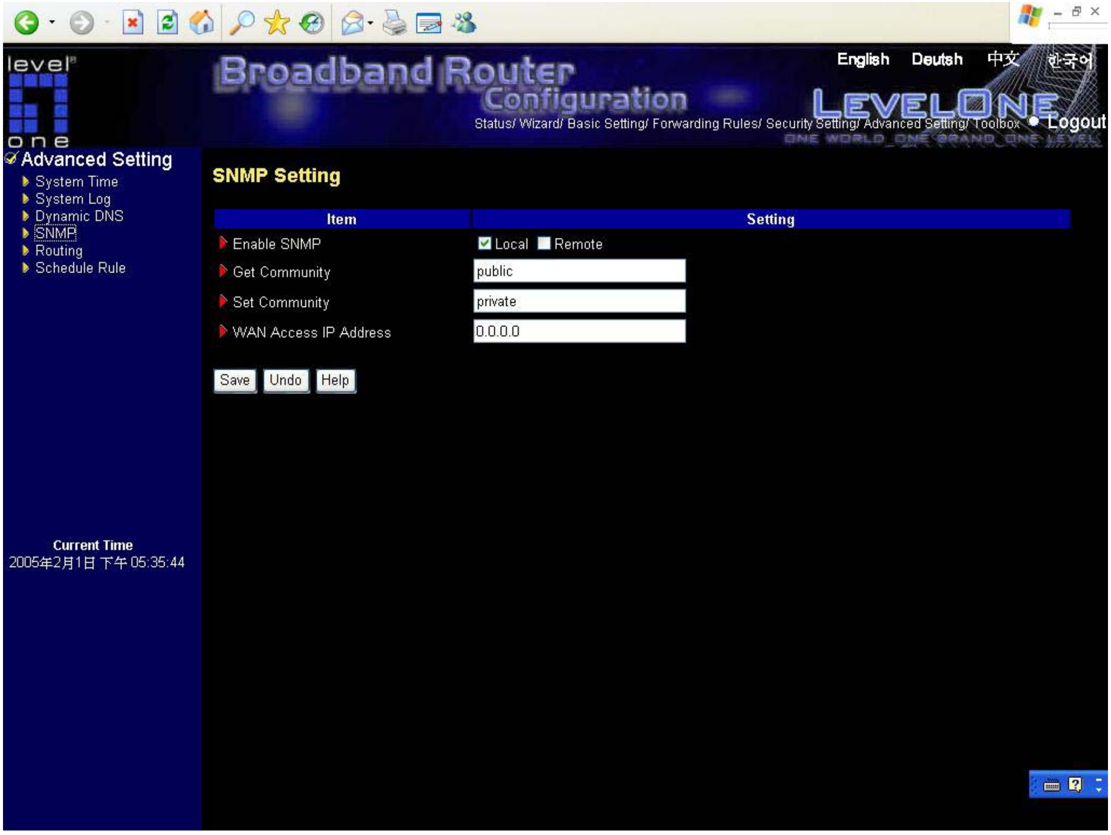
| Item | Setting |
|---|---|
| DDNS | ○ Disable ● Enable |
| Provider | DynDNS.org(Dynamic) |
| Host Name | levelone.dyndns.org |
| Username / E-mail | ss@levelone.com |
| Password / Key | ************ |

Current Time
06/04/2004 03:47:53

After Dynamic DNS setting is configured, click the save button.

The new settings will be effective after reboot.

## 4.7.4 SNMP Setting


Broadband Router Configuration
English Deutsh 中文 한국어
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Undo
Help

SNMP Setting

| Item | Setting |
|---|---|
| Enable SNMP | ☑ Local □ Remote |
| Get Community | public |
| Set Community | private |
| WAN Access IP Address | 0.0.0.0 |

Current Time
2005年2月1日 下午 05:35:44

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

**Enable SNMP**

You must check either Local or Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

**Get Community**

Setting the community of GetRequest your device will response.

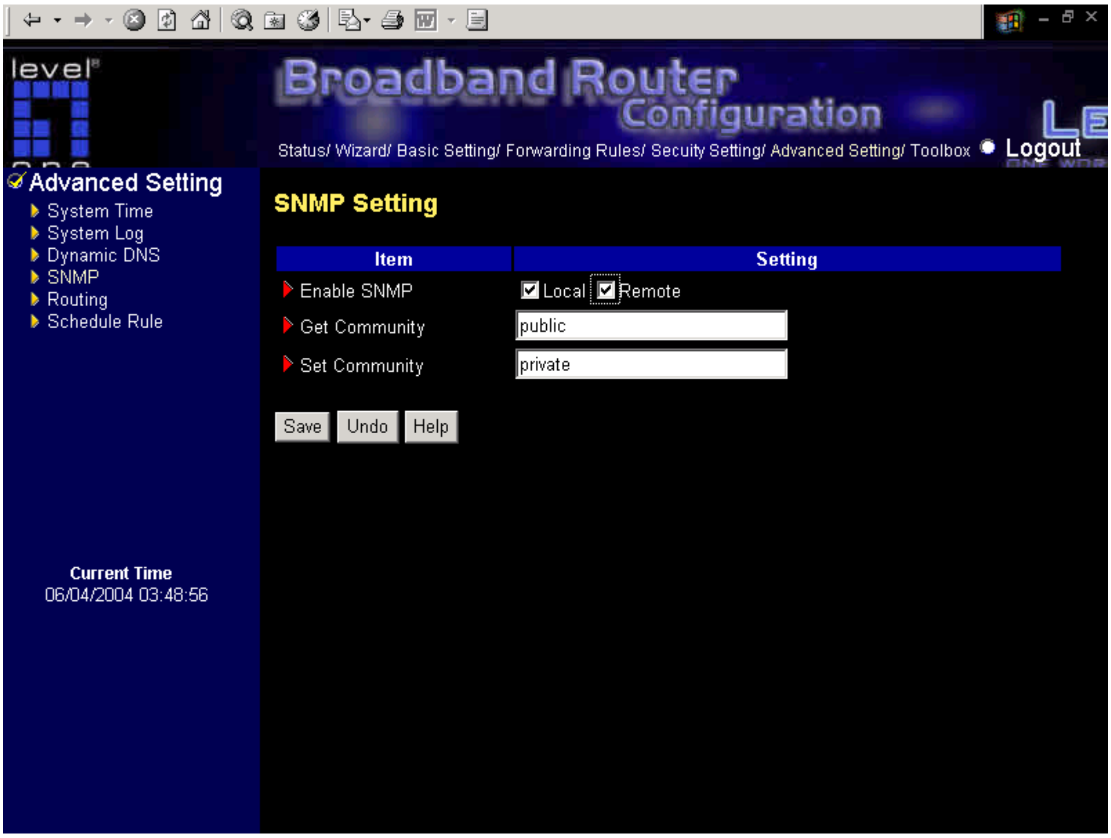
**Set Community**

Setting the community of SetRequest your device will accept.

**WAN Access IP Address**

WBR-5400 will only respond the SNMP packet to the device with the entered IP.
If left it blank, WBR-5400 will not respond SNMP packet from WAN port.

**Example:**



Broadband Router Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Current Time
06/04/2004 03:48:56

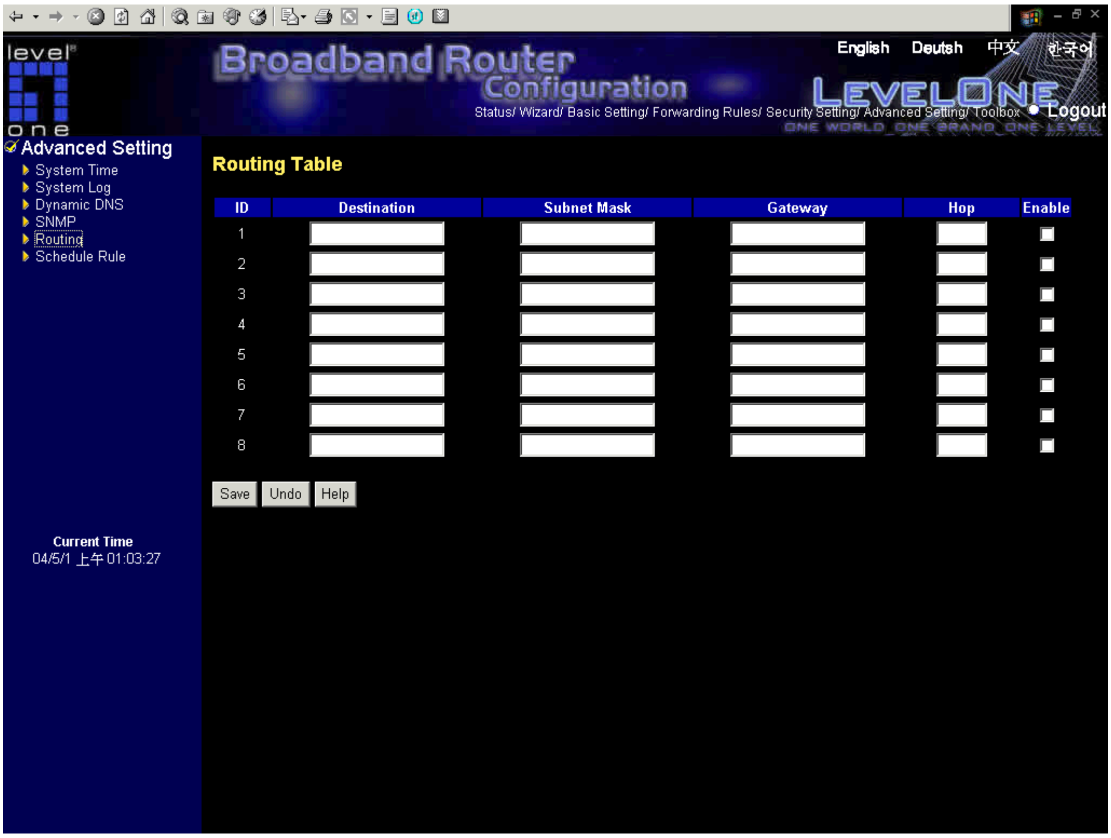
SNMP Setting

| Item | Setting |
|---|---|
| Enable SNMP | ☑ Local ☑ Remote |
| Get Community | public |
| Set Community | private |

1. This device will response to SNMP client which’s **get community** is set as “public”

2. This device will response to SNMP client which’s **set community** is set as “private”

## 4.7.5 Routing Table


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Undo
Help

Current Time
04/5/1 上午 01:03:27

Routing Table

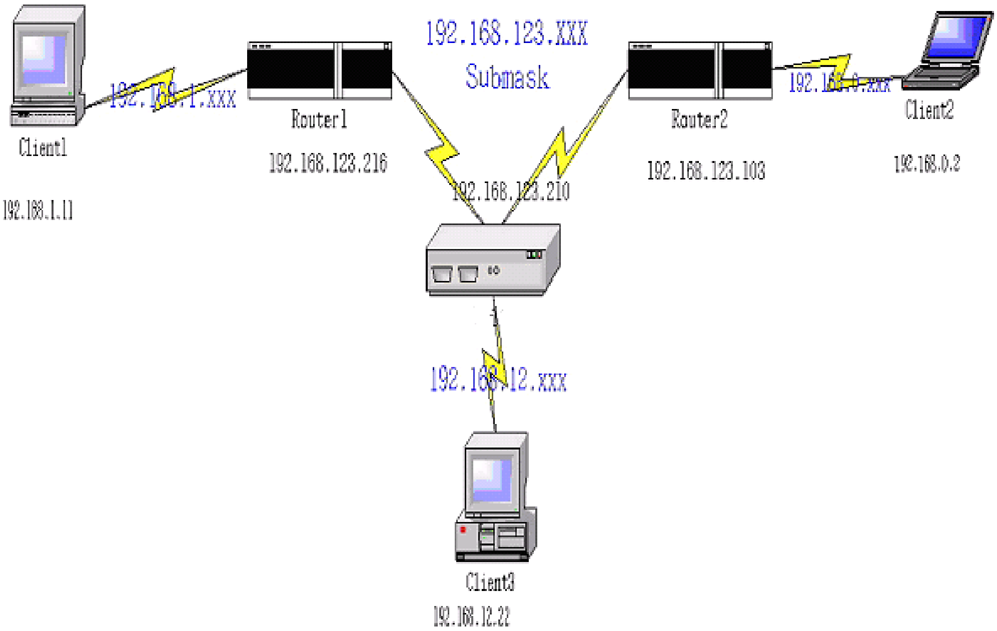
| ID | Destination | Subnet Mask | Gateway | Hop | Enable |
|---|---|---|---|---|---|
| 1 | | | | | □ |
| 2 | | | | | □ |
| 3 | | | | | □ |
| 4 | | | | | □ |
| 5 | | | | | □ |
| 6 | | | | | □ |
| 7 | | | | | □ |
| 8 | | | | | □ |

**Routing Tables** allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static.

**Static Routing**: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

**Example:**



Configuration on NAT Router

| Destination | SubnetMask | Gateway | Hop | Enabled |
|---|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.123.216 | 1 | V |
| 192.168.0.0 | 255.255.255.0 | 192.168.123.103 | 1 | V |

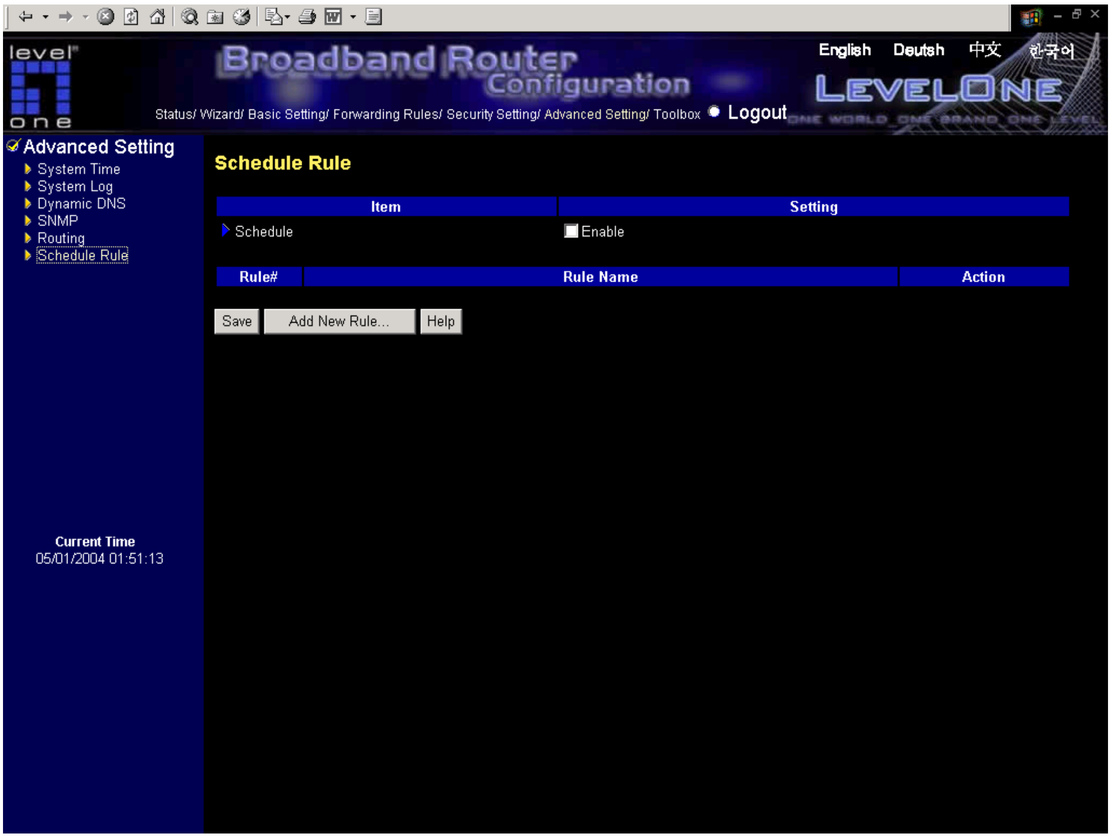
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

### 4.7.6 Schedule Rule


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Add New Rule...
Help

Schedule Rule

| Item | Setting |
|---|---|
| Schedule | □ Enable |

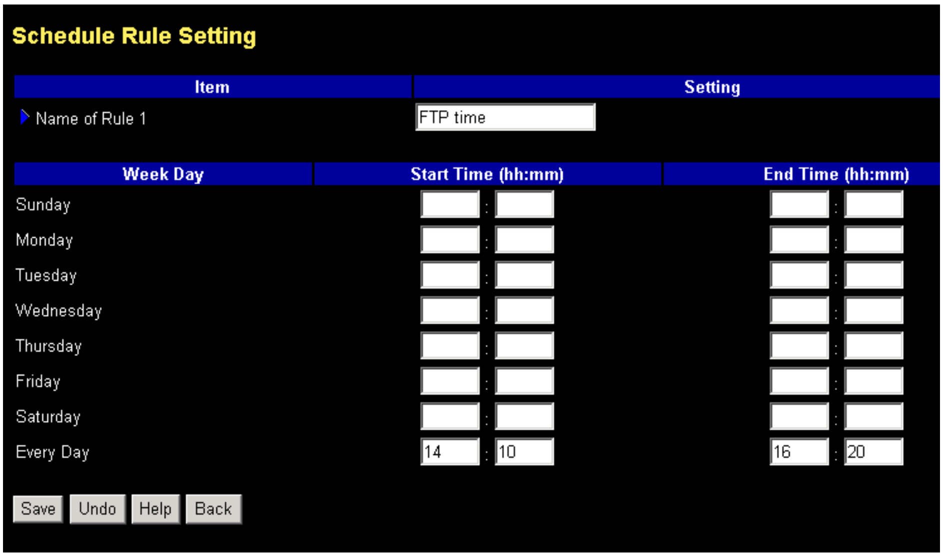
| Rule# | Rule Name | Action |
|---|---|---|

Current Time
05/01/2004 01:51:13

You can set the schedule time to decide which service will be turned on or off. Select the "enable" item.

Press **"Add New Rule"**

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20

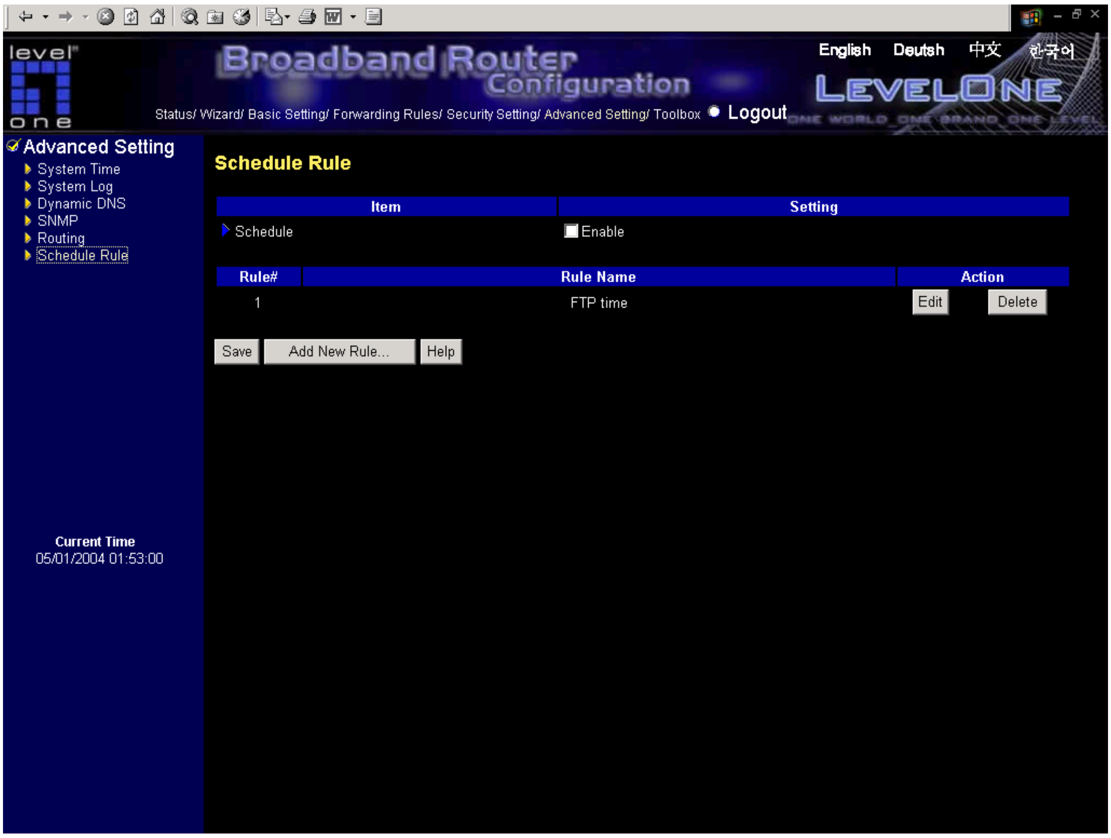


## Schedule Rule Setting

| Item | Setting |
|---|---|
| Name of Rule 1 | FTP time |

| Week Day | Start Time (hh:mm) | End Time (hh:mm) |
|---|---|---|
| Sunday | : | : |
| Monday | : | : |
| Tuesday | : | : |
| Wednesday | : | : |
| Thursday | : | : |
| Friday | : | : |
| Saturday | : | : |
| Every Day | 14 : 10 | 16 : 20 |

**After configure Rule 1→**


Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Save
Add New Rule...
Help

Schedule Rule

| Item | Setting |
|---|---|
| Schedule | □ Enable |

| Rule# | Rule Name | Action |
|---|---|---|
| 1 | FTP time | Edit Delete |

Current Time
05/01/2004 01:53:00

**Schedule Enable**

Selected if you want to Enable the Scheduler.

**Edit**

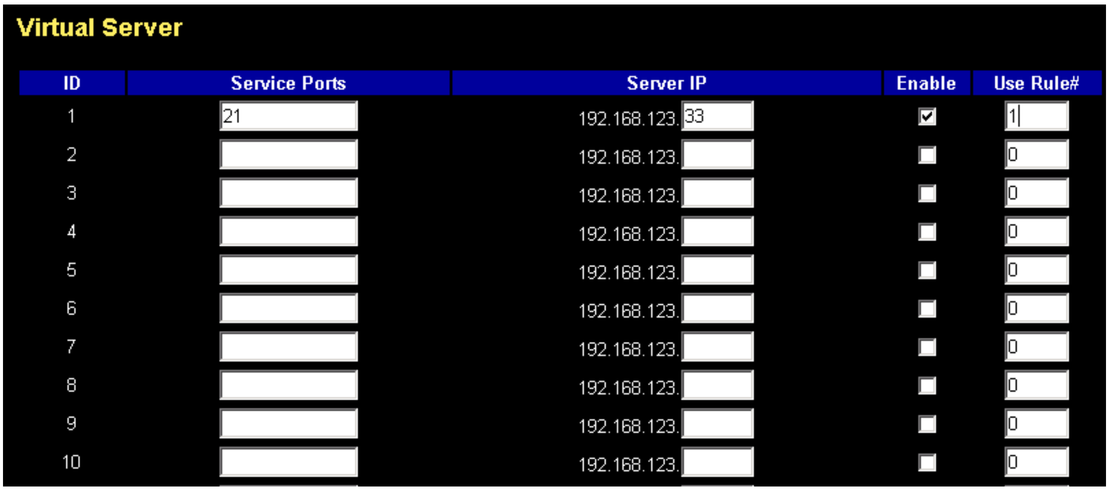
To edit the schedule rule.

**Delete**

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

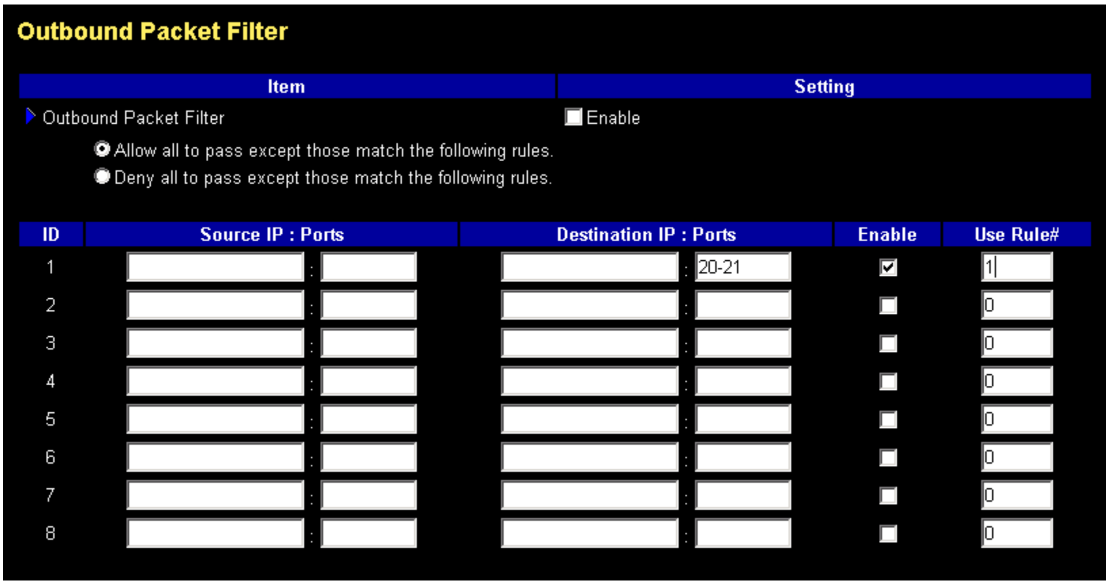
Exanple1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)



## Virtual Server

| ID | Service Ports | Server IP | Enable | Use Rule# |
|---|---|---|---|---|
| 1 | 21 | 192.168.123.33 | ☑ | 1 |
| 2 |  | 192.168.123. | □ | 0 |
| 3 |  | 192.168.123. | □ | 0 |
| 4 |  | 192.168.123. | □ | 0 |
| 5 |  | 192.168.123. | □ | 0 |
| 6 |  | 192.168.123. | □ | 0 |
| 7 |  | 192.168.123. | □ | 0 |
| 8 |  | 192.168.123. | □ | 0 |
| 9 |  | 192.168.123. | □ | 0 |
| 10 |  | 192.168.123. | □ | 0 |

Exanple2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).



## Outbound Packet Filter

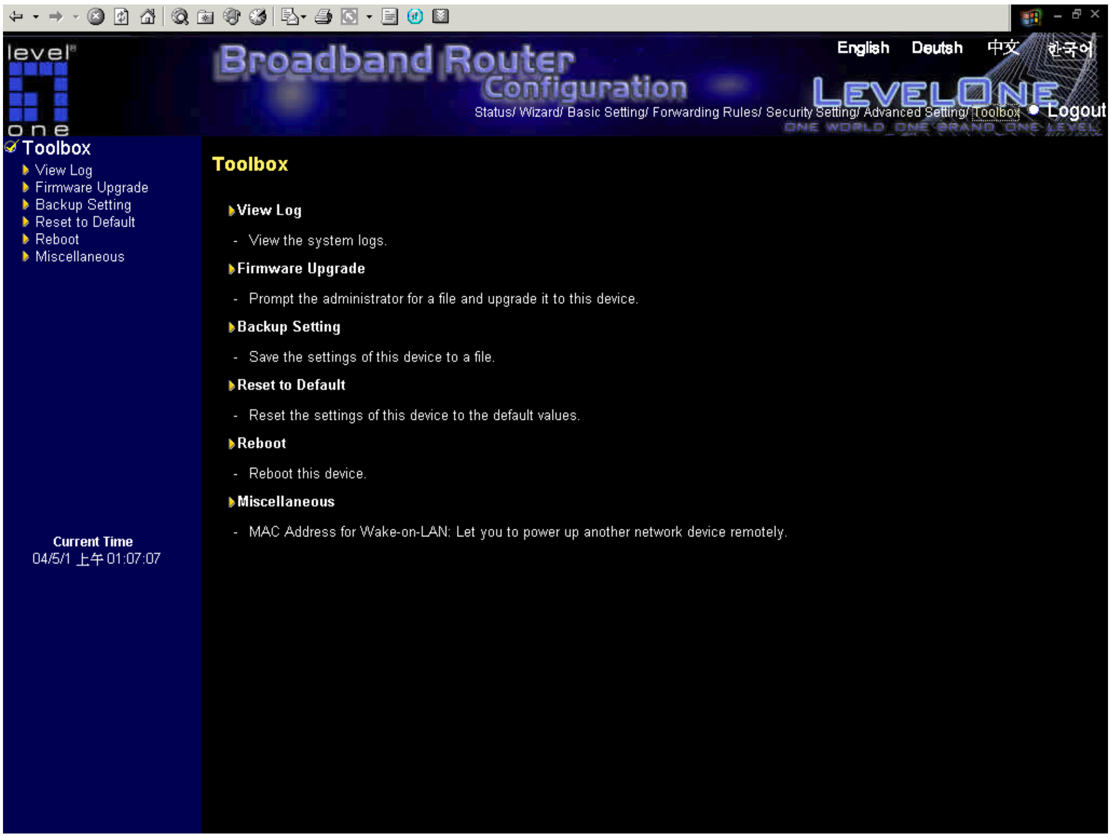
| Item | Setting |
|---|---|
| Outbound Packet Filter | □ Enable |

● Allow all to pass except those match the following rules.

○ Deny all to pass except those match the following rules.

| ID | Source IP : Ports | | Destination IP : Ports | | Enable | Use Rule# |
|---|---|---|---|---|---|---|
| 1 |  |  |  | 20-21 | ☑ | 1 |
| 2 |  |  |  |  | □ | 0 |
| 3 |  |  |  |  | □ | 0 |
| 4 |  |  |  |  | □ | 0 |
| 5 |  |  |  |  | □ | 0 |
| 6 |  |  |  |  | □ | 0 |
| 7 |  |  |  |  | □ | 0 |
| 8 |  |  |  |  | □ | 0 |

## 4.8 Toolbox



**Toolbox**

**View Log**

- View the system logs.

**Firmware Upgrade**

- Prompt the administrator for a file and upgrade it to this device.

**Backup Setting**

- Save the settings of this device to a file.

**Reset to Default**

- Reset the settings of this device to the default values.

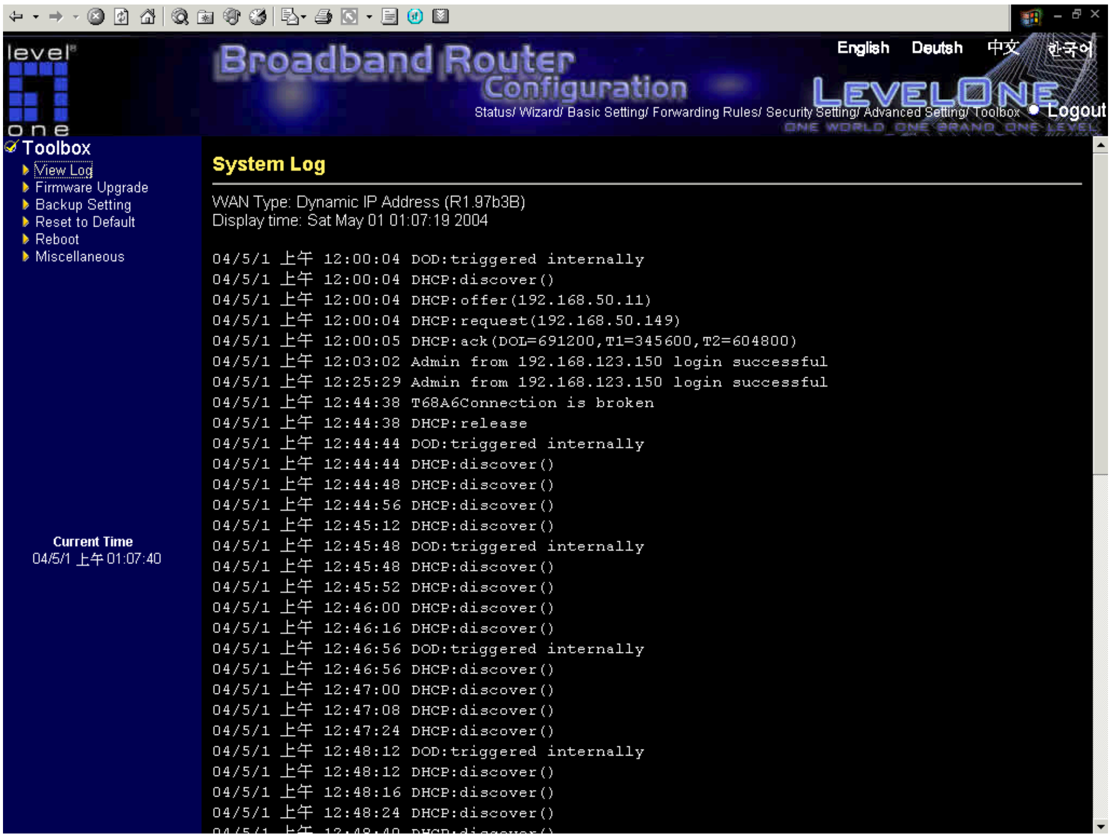
**Reboot**

- Reboot this device.

**Miscellaneous**

- MAC Address for Wake-on-LAN: Let you to power up another network device remotely.

### 4.8.1 System Log


Broadband Router Configuration
English
Deutsh
中文
한국어
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous

Current Time
04/5/1 上午 01:07:40

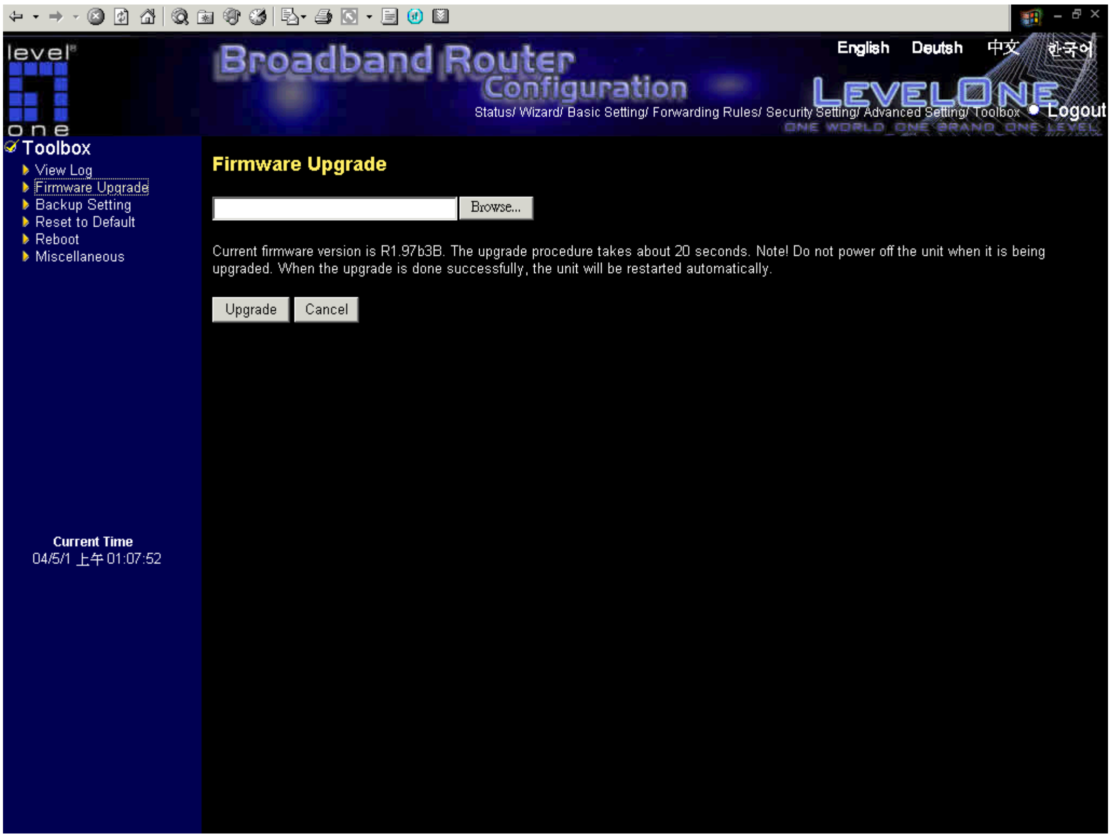
System Log

WAN Type: Dynamic IP Address (R1.97b3B)
Display time: Sat May 01 01:07:19 2004

```
04/5/1 上午 12:00:04 DOD:triggered internally
04/5/1 上午 12:00:04 DHCP:discover()
04/5/1 上午 12:00:04 DHCP:offer(192.168.50.11)
04/5/1 上午 12:00:04 DHCP:request(192.168.50.149)
04/5/1 上午 12:00:05 DHCP:ack(DOL=691200,T1=345600,T2=604800)
04/5/1 上午 12:03:02 Admin from 192.168.123.150 login successful
04/5/1 上午 12:25:29 Admin from 192.168.123.150 login successful
04/5/1 上午 12:44:38 T68A6Connection is broken
04/5/1 上午 12:44:38 DHCP:release
04/5/1 上午 12:44:44 DOD:triggered internally
04/5/1 上午 12:44:44 DHCP:discover()
04/5/1 上午 12:44:48 DHCP:discover()
04/5/1 上午 12:44:56 DHCP:discover()
04/5/1 上午 12:45:12 DHCP:discover()
04/5/1 上午 12:45:48 DOD:triggered internally
04/5/1 上午 12:45:48 DHCP:discover()
04/5/1 上午 12:45:52 DHCP:discover()
04/5/1 上午 12:46:00 DHCP:discover()
04/5/1 上午 12:46:16 DHCP:discover()
04/5/1 上午 12:46:56 DOD:triggered internally
04/5/1 上午 12:46:56 DHCP:discover()
04/5/1 上午 12:47:00 DHCP:discover()
04/5/1 上午 12:47:08 DHCP:discover()
04/5/1 上午 12:47:24 DHCP:discover()
04/5/1 上午 12:48:12 DOD:triggered internally
04/5/1 上午 12:48:12 DHCP:discover()
04/5/1 上午 12:48:16 DHCP:discover()
04/5/1 上午 12:48:24 DHCP:discover()
04/5/1 上午 12:48:40 DHCP:discover()
```

You can View system log by clicking the **View Log** button

### 4.8.2 Firmware Upgrade

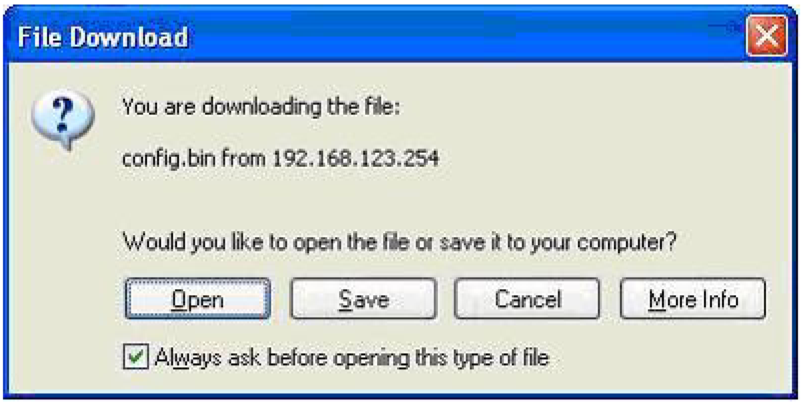


level one
Broadband Router Configuration
English Deutsh 中文 한국어
LEVELONE
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
ONE WORLD ONE BRAND ONE LEVEL
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Current Time
04/5/1 上午 01:07:52
Firmware Upgrade
Browse...
Upgrade
Cancel

Current firmware version is R1.97b3B. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

You can upgrade firmware by clicking **Firmware Upgrade** button.

### 4.8.3 Backup Setting



You are downloading the file:

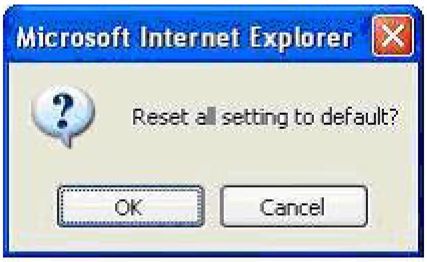
config.bin from 192.168.123.254

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

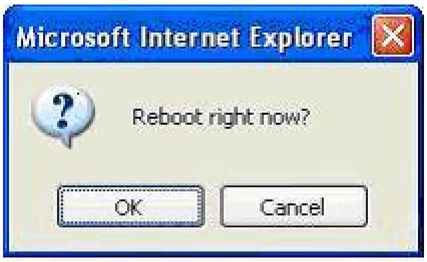
### 4.8.4 Reset to default



Reset all setting to default?

You can also reset this product to factory default by clicking the **Reset to default** button.

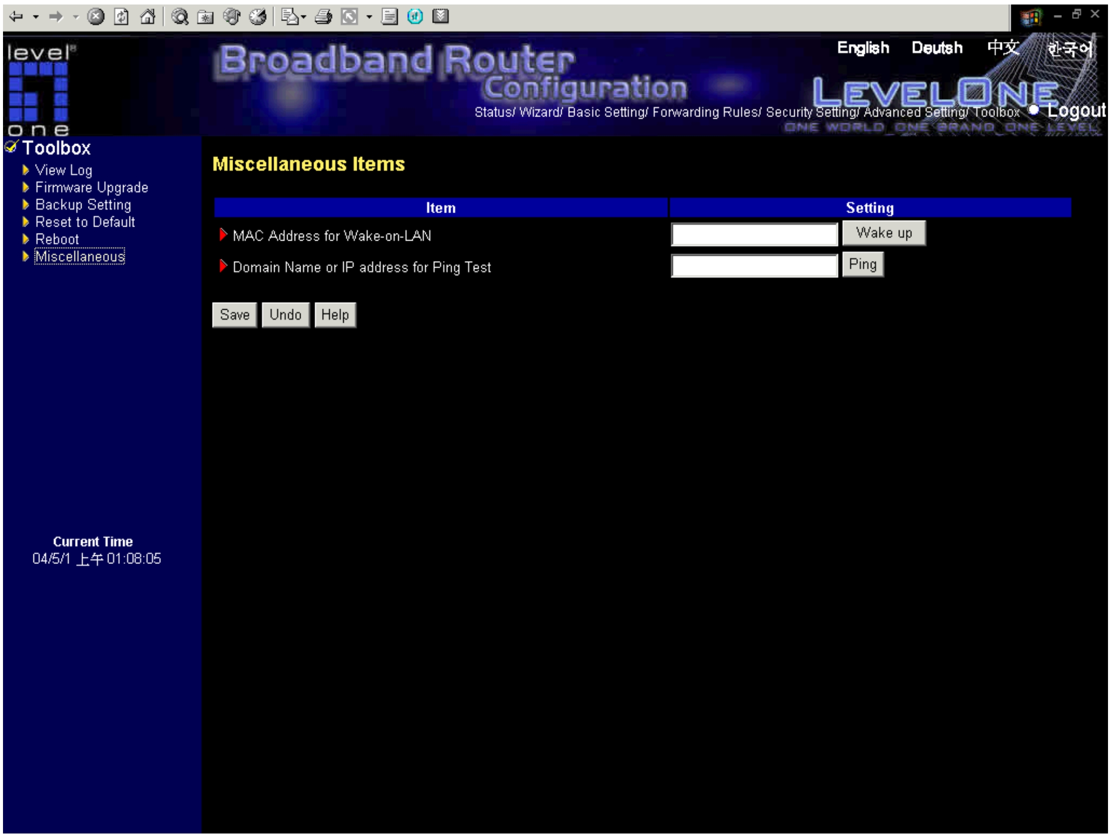
### 4.8.5 Reboot



Reboot right now?

You can also reboot this product by clicking the **Reboot** button.

### 4.8.6 Miscellaneous Items



Miscellaneous Items

| Item | Setting |
|---|---|
| MAC Address for Wake-on-LAN | Wake up |
| Domain Name or IP address for Ping Test | Ping |

### MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

### Domain Name or IP address for Ping Test

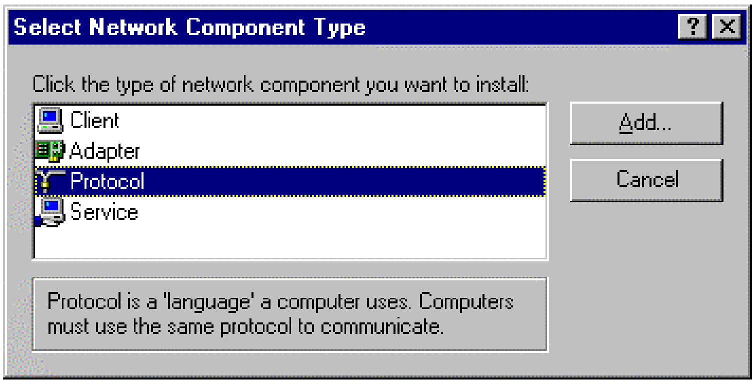
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

# Appendix A TCP/IP Configuration for Windows 95/98

This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

### A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



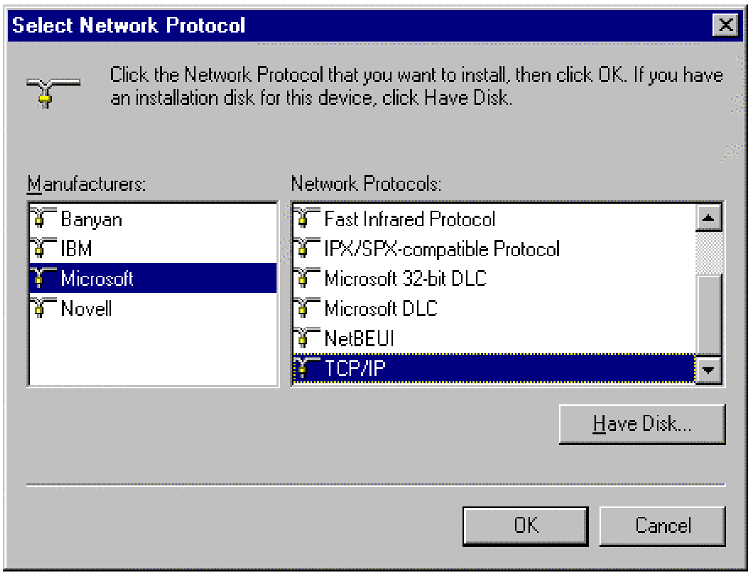
Select Network Component Type

Click the type of network component you want to install:

Protocol

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

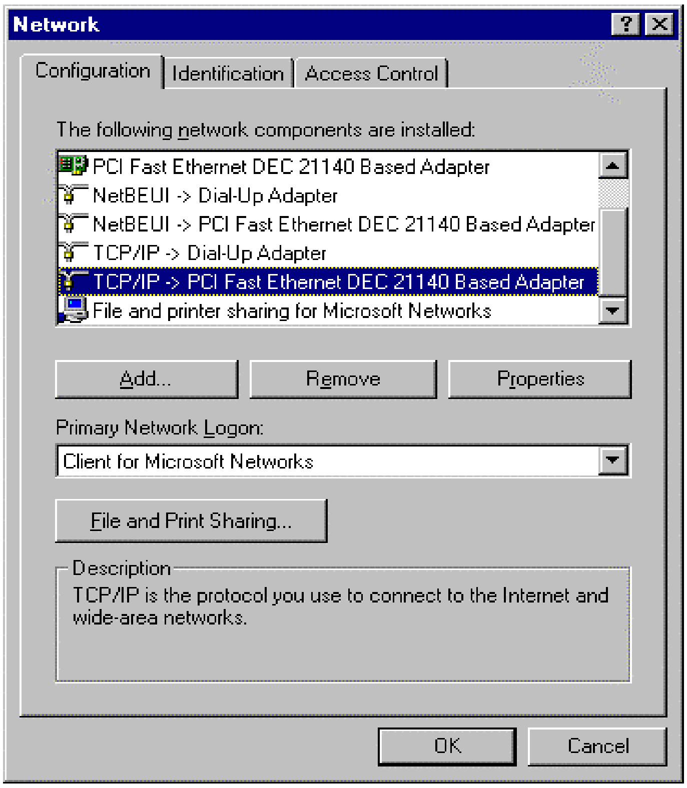
Manufacturers: Microsoft

Network Protocols: TCP/IP

6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

## A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.



The following network components are installed:

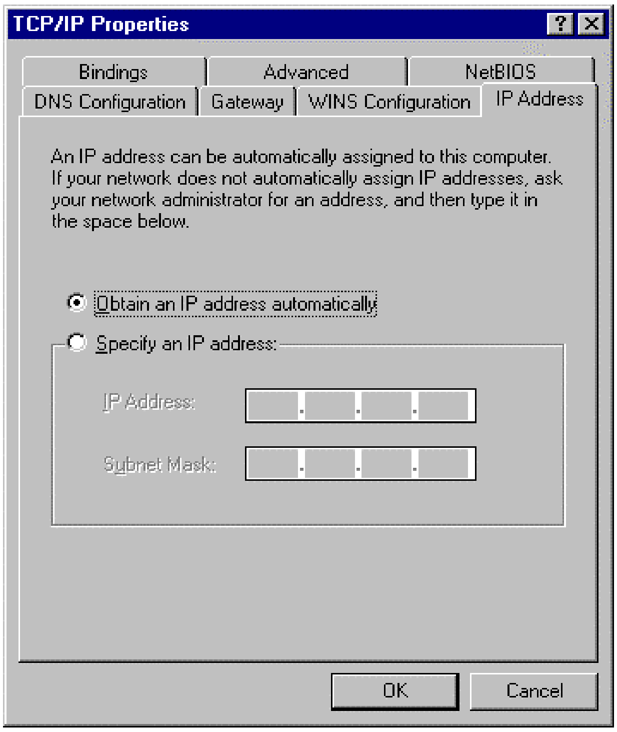
PCI Fast Ethernet DEC 21140 Based Adapter
NetBEUI -> Dial-Up Adapter
NetBEUI -> PCI Fast Ethernet DEC 21140 Based Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> PCI Fast Ethernet DEC 21140 Based Adapter
File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:

a. Select **Obtain an IP address automatically** in the IP Address tab.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

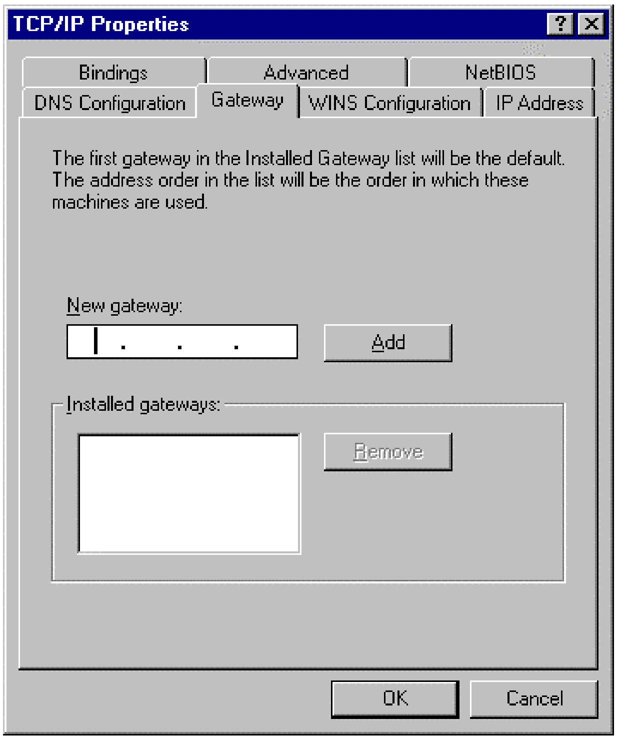
● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

b. Don't input any value in the Gateway tab.

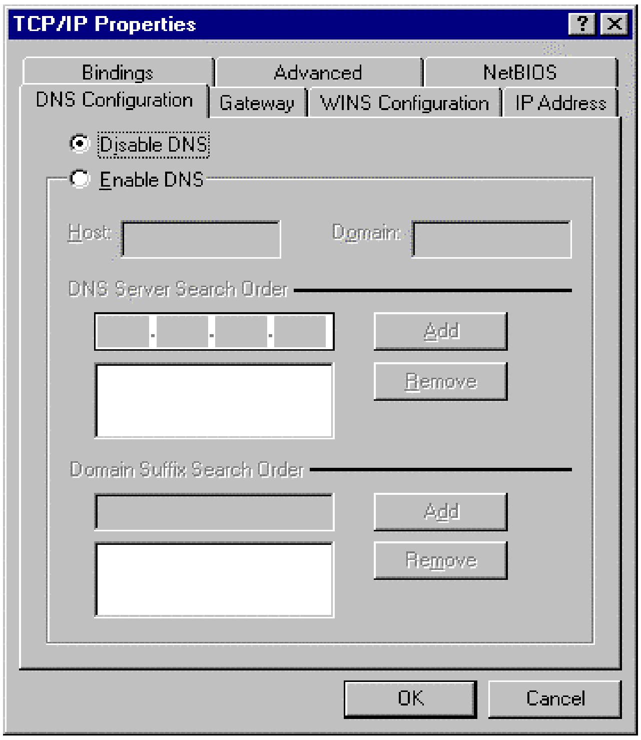


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: . . .

Installed gateways:

c. Choose **Disable DNS** in the DNS Configuration tab.

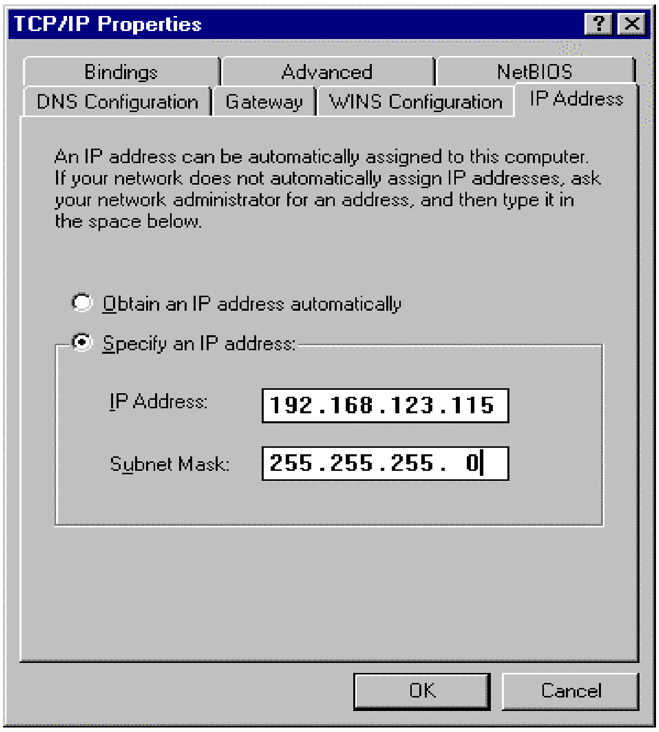


● Disable DNS

○ Enable DNS

B. Configure IP manually

a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

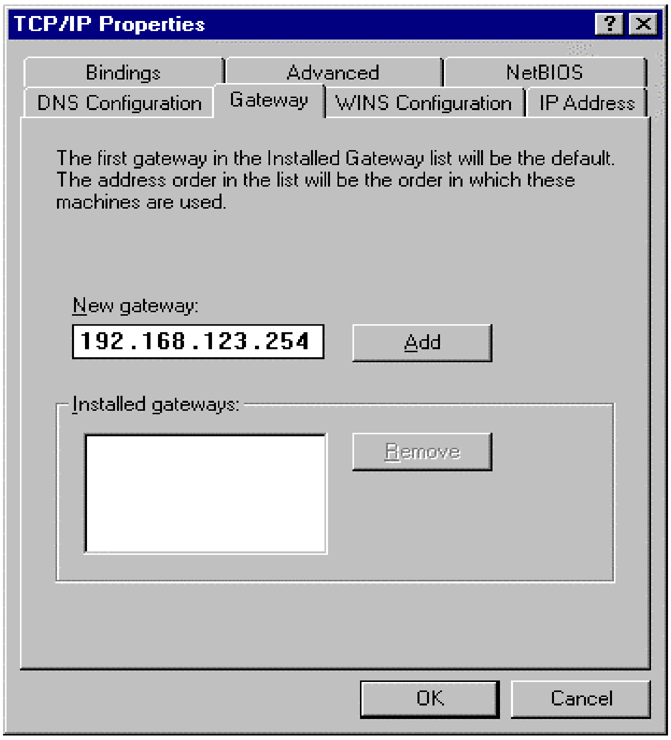
○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168.123.115

Subnet Mask: 255.255.255. 0

b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.

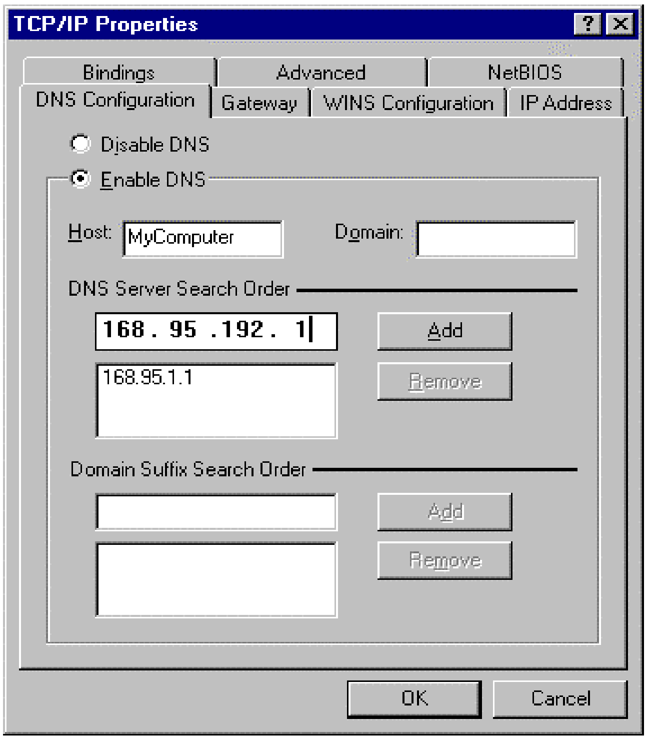


TCP/IP Properties

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.123.254

c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.



TCP/IP Properties

○ Disable DNS

● Enable DNS

Host: MyComputer

Domain:

DNS Server Search Order: 168 . 95 .192 . 1

168.95.1.1

# Appendix B 802.1x Setting

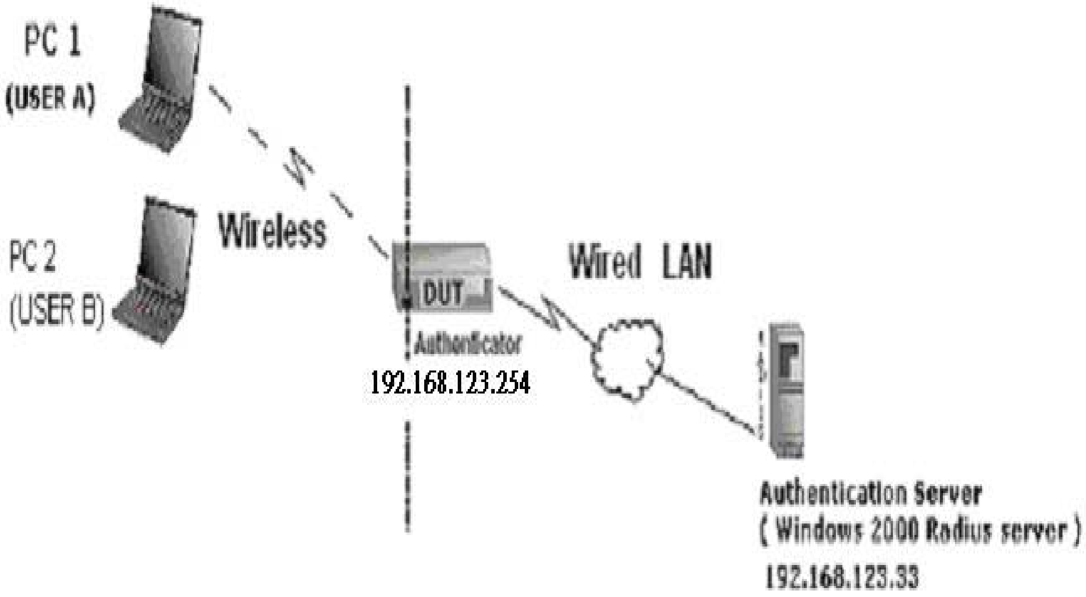


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

**1 Equipment Details**

PC1 OS:

Microsoft Windows XP Professional without Service Pack 1.

PC2 OS:

Microsoft Windows XP Professional with Service Pack 1a.

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 *(You can get more information from http://support.microsoft.com/default.aspx?scid=kb; en-us;313664)*

**2 DUT**

**Configuration:**

1.Enable DHCP server.

2.WAN setting: static IP address.

3.LAN IP address: 192.168.123.254/24.

4.Set RADIUS server IP.

5.Set RADIUS server shared key.

6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

## 3. DUT and Windows 2000 Radius Server Setup

3-1-1. Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

3-1-2. Setup DUT

1.Enable the 802.1X (check the "Enable checkbox").

2.Enter the RADIUS server IP.

3.Enter the shared key. (The key shared by the RADIUS server and DUT).

4.We will change 802.1X encryption key length to fit the variable test condition.

3-1-3. Setup Network adapter on PC

1.Choose the IEEE802.1X as the authentication method. (Fig 2)

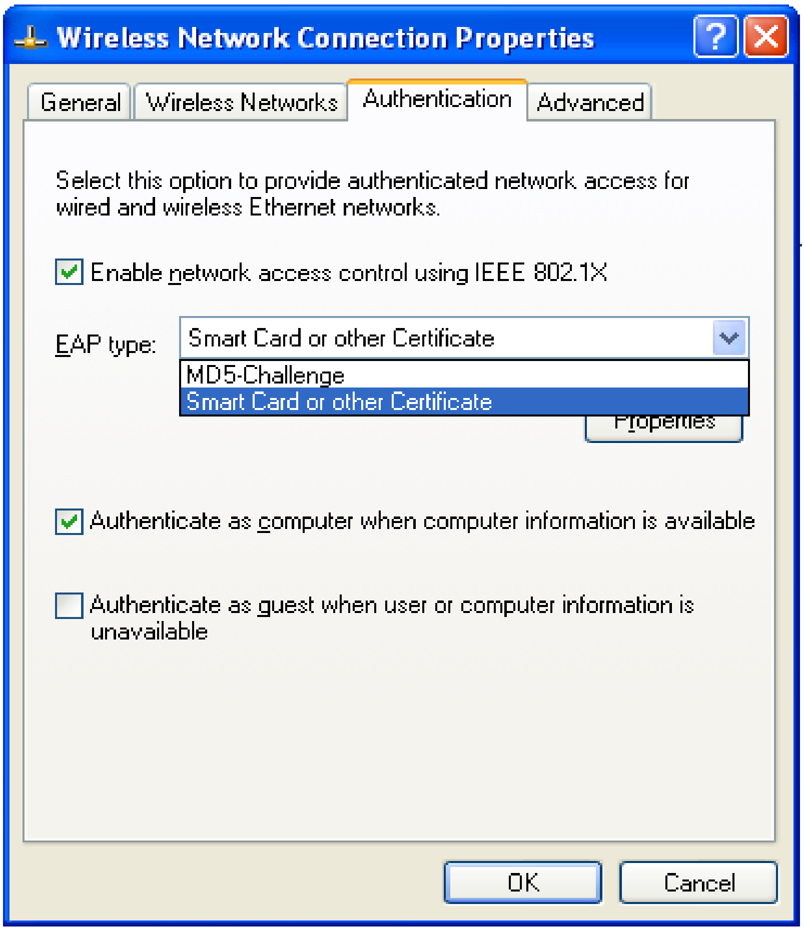
Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

2.Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.

3.If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)

4. We will change EAP type to fit the variable test condition.



Wireless Network Connection Properties

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: Smart Card or other Certificate

MD5-Challenge
Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

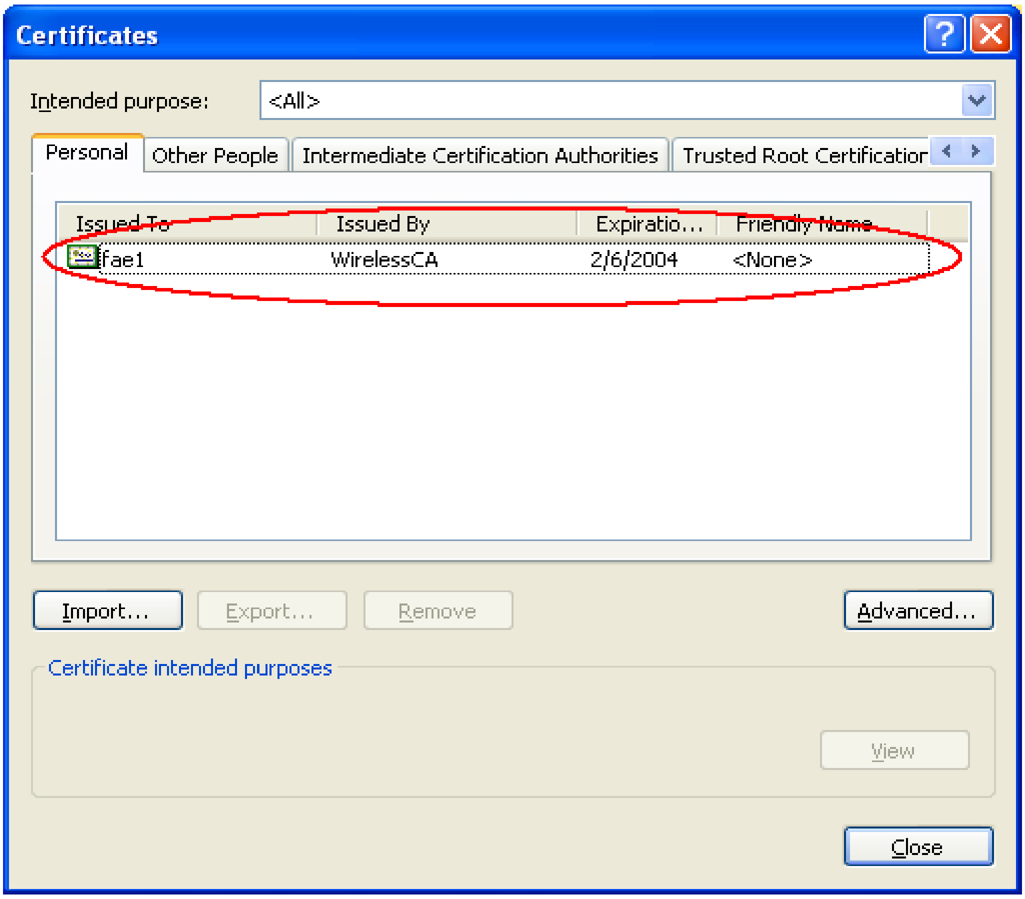
**Figure 2: Enable IEEE 802.1X access control**

**Figure 3: Smart card or certificate properties**

## 4. Windows 2000 RADIUS server Authentication testing:

4.1DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

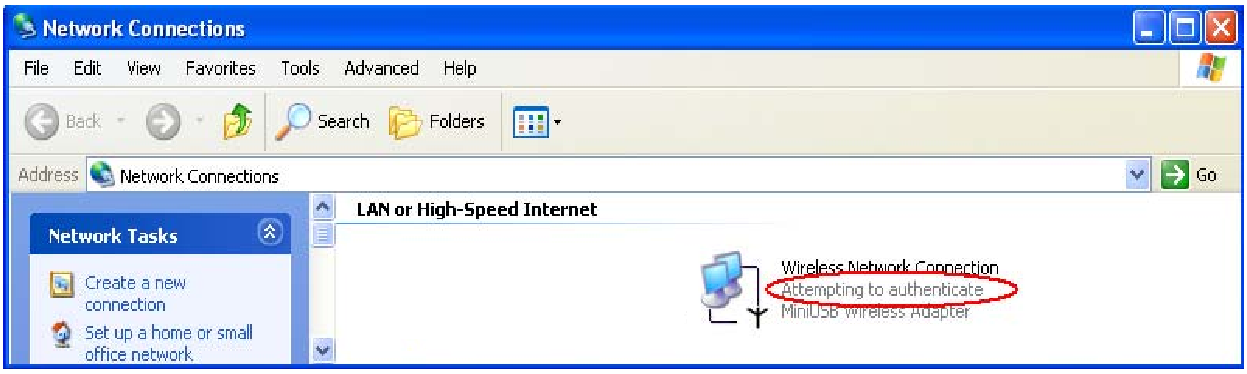
1. Download and install the certificate on PC1. (Fig 4)
2. PC1 choose the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. ( Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| fae1 | WirelessCA | 2/6/2004 | <None> |

Figure 4: Certificate information on PC1

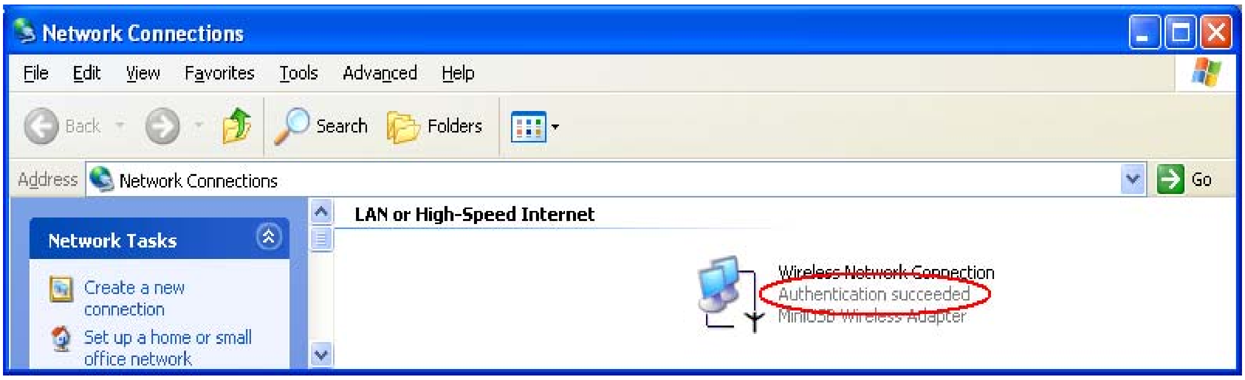


Address: Network Connections

LAN or High-Speed Internet

Wireless Network Connection
Attempting to authenticate
MiniUSB Wireless Adapter

Figure 5: Authenticating



Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
LAN or High-Speed Internet

Wireless Network Connection
Authentication succeeded
MiniUSB Wireless Adapter

**Figure 6: Authentication success**

**4.2**DUT authenticate PC2 using PEAP-TLS.

1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.

4.The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.

5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

**Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.**

Note.

1.PC1 is on Windows XP platform without Service Pack 1.

2.PC2 is on Windows XP platform with Service Pack 1a.

3.PEAP is supported on Windows XP with Service Pack 1 only.

4.Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

# Appendix C　Reset to factory default

## Reset to factory Default

There are 2 methods to reset to default.

1. **Restore with RESET button**

First, turn off the router and press the RESET button in. And then, power on the router and push the RESET button down until the Status LED start flashing, then remove the finger. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

2. **Restore directly when the router power on**

First, push the RESET button about 5 seconds , and STATUS will start flashing about 5 times), remove the finger.

. The RESTORE process is completed.